

Integrating Novell®
Open Enterprise Server for Linux

COURSE 3077

Novell Training Services

www.novell.com

AUTHORIZED COURSEWARE

Volume 2

Part # 100-005076-001
Version 1

Novell®

Proprietary Statement

Copyright © 2005 Novell, Inc. All rights reserved.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express prior consent of the publisher. This manual, and any portion thereof, may not be copied without the express written permission of Novell, Inc.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606-2399

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to revise this publication and to make changes in its content at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any NetWare software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to make changes to any and all parts of NetWare software at any time, without obligation to notify any person or entity of such changes.

This Novell Training Manual is published solely to instruct students in the use of Novell networking software. Although third-party application software packages are used in Novell training courses, this is for demonstration purposes only and shall not constitute an endorsement of any of these software applications.

Further, Novell, Inc. does not represent itself as having any particular expertise in these application software packages and any use by students of the same shall be done at the students' own risk.

Software Piracy

Throughout the world, unauthorized duplication of software is subject to both criminal and civil penalties.

If you know of illegal copying of software, contact your local Software Antipiracy Hotline.

For the Hotline number for your area, access Novell's World Wide Web page at http://www.novell.com and look for the piracy page under "Programs."

Or, contact Novell's anti-piracy headquarters in the U.S. at 800-PIRATES (747-2837) or 801-861-7101.

Trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell, Inc. Trademarks

Novell, the Novell logo, NetWare, BorderManager, ConsoleOne, DirXML, GroupWise, iChain, ManageWise, NDPS, NDS, NetMail, Novell Directory Services, Novell iFolder, Novell SecretStore, Ximian, Ximian Evolution and ZENworks are registered trademarks; CDE, Certified Directory Engineer and CNE are registered service marks; eDirectory, Evolution, exteNd, exteNd Composer, exteNd Directory, exteNd Workbench, Mono, NIMS, NLM, NMAS, Novell Certificate Server, Novell Client, Novell Cluster Services, Novell Distributed Print Services, Novell Internet Messaging System, Novell Storage Services, Nsure, Nsure Resources, Nterprise, Nterprise Branch Office, Red Carpet and Red Carpet Enterprise are trademarks; and Certified Novell Administrator, CNA, Certified Novell Engineer, Certified Novell Instructor, CNI, Master CNE, Master CNI, MCNE, MCNI, Novell Education Academic Partner, NEAP, Ngage, Novell Online Training Provider, NOTP and Novell Technical Services are service marks of Novell, Inc. in the United States and other countries. SUSE is a registered trademark of SUSE LINUX AG, a Novell company. For more information on Novell trademarks, please visit http://www.novell.com/company/legal/trademarks/tmlist.html.

Other Trademarks

Adaptec is a registered trademark of Adaptec, Inc. AMD is a trademark of Advanced Micro Devices. AppleShare and AppleTalk are registered trademarks of Apple Computer, Inc. ARCserv is a registered trademark of Cheyenne Software, Inc. Btrieve is a registered trademark of Pervasive Software, Inc. EtherTalk is a registered trademark of Apple Computer, Inc. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds. LocalTalk is a registered trademark of Apple Computer, Inc. Lotus Notes is a registered trademark of Lotus Development Corporation. Macintosh is a registered trademark of Apple Computer, Inc. Netscape Communicator is a trademark of Netscape Communications Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. Pentium is a registered trademark of Intel Corporation. Solaris is a registered trademark of Sun Microsystems, Inc. The Norton AntiVirus is a trademark of Symantec Corporation. TokenTalk is a registered trademark of Apple Computer, Inc. Tru64 is a trademark of Digital Equipment Corp. UnitedLinux is a registered trademark of UnitedLinux. UNIX is a registered trademark of the Open Group. WebSphere is a trademark of International Business Machines Corporation. Windows and Windows NT are registered trademarks of Microsoft Corporation.

All other third-party trademarks are the property of their respective owners.

Contents

Introduction

Student Kit Deliverables Intro-2

Course Design Intro-3

- Course Objectives Intro-3
- Course Audience Intro-4
- Prerequisite Knowledge Intro-6
- Certification Intro-7
- Novell Open Enterprise Server Training Path Intro-7
- Classroom Agenda Intro-8
- Course Setup Intro-9

Exercise Guidelines Intro-10

- VMware and the Exercises Intro-10
- Exercise Conventions Intro-18
- Self-Study Setup Intro-19
- Novell Open Enterprise Server Product Documentation . Intro-19
- Web Browser Tools and Applications Intro-19
- Scenario Intro-20

Course Feedback Intro-21

SECTION 1 Evaluate and Upgrade to Novell Open Enterprise Server

Objectives 1-1

Introduction 1-2

Objective 1 Describe Novell Open Enterprise Server (OES) 1-3

- Why Upgrade to Novell OES 1-5
- Novell OES Features 1-9

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective 2 Decide Which OES Services to Install 1-15
What Services Are Included in OES? 1-15
Which Services Do I Need? 1-19
Which OES Platform Is Best for My Services? 1-20

Objective 3 Plan Your OES Implementation 1-29
Plan for eDirectory 1-29
Prepare Your Existing eDirectory Tree for OES 1-33
Identify a Purpose for Each Server 1-33
Evaluate Server Requirements 1-34
Evaluate User Restrictions and Linux User Management . . . 1-38
Consider Coexistence and Migration Issues 1-39
Review Your Installation Options Before You Start 1-39

Objective 4 Purchase and License Novell OES 1-47
How to Get OES Through Upgrade Protection 1-47
How to Purchase OES 1-47
Novell OES Licensing 1-48

Objective 5 Upgrade to Novell OES NetWare 1-51
Review Upgrade Guidelines Options for OES NetWare 1-52
Check System Requirements 1-55
Determine the Services to Install 1-57
Verify Rights for Upgrading to OES NetWare 1-59
Prepare the Network with Deployment Manager 1-61
Prepare the Computer 1-63
Start an In-Place Server Upgrade 1-65
Complete the OES NetWare Server Upgrade 1-67
Complete Post-Installation Tasks 1-74
Exercise **1-1** Upgrade to Novell OES NetWare 1-75

Summary 1-76

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

SECTION 2 Manage an OES Linux Server

Objectives 2-1

Introduction 2-2

Objective 1 Manage an OES Linux Server from the KDE Desktop 2-3

- What the root User Is 2-3
- How to Log In 2-4
- How to Log Out 2-5
- How to Shut Down and Reboot the Linux System 2-6
- How to Identify KDE Desktop Components 2-7
- How to Use the Konqueror File Manager 2-10
- Exercise **2-1** Manage Your OES Linux Server from the KDE Desktop 2-14

Objective 2 Perform Administrative Tasks with YaST 2-15

- Exercise **2-2** Configure an OES Linux Server with YaST 2-23

Objective 3 Manage an OES Server from a Bash Shell 2-24

- Virtual Consoles on OES Linux 2-24
- Bash Shell on OES Servers 2-26
- Bash Shell and OES NetWare 2-34
- Common Bash File System Commands 2-35
- Bash Command Web References 2-37
- NetWare Commands and Linux Equivalents 2-37
- Exercise **2-3** Manage OES Linux Servers from a Command Prompt 2-60

Objective 4 Manage the Linux File System 2-61

- Linux File System Types 2-61
- The Hierarchical Structure of the File System 2-64
- FHS (Filesystem Hierarchy Standard) 2-65
- Root Directory (/) 2-66
- Storage Devices 2-67
- File System Mount Points 2-68
- User Directories (/home/) 2-72
- Filename Restrictions 2-72
- Linux File System Permissions 2-73
- Exercise **2-4** Manage Linux Files and Directories 2-82

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Summary 2-83

SECTION 3 Manage Novell OES Servers

Objectives 3-1

Introduction 3-2

Objective 1 Manage OES Servers Remotely with OpenSSH 3-5

Benefits of OpenSSH 3-5
OpenSSH and OES Linux 3-6
OpenSSH and OES NetWare 3-9
How to Use SSH Commands 3-11
Exercise **3-1** Manage OES Servers Remotely with OpenSSH . 3-16

Objective 2 Manage OES Servers with Novell Remote Manager (NRM) .3-17

NRM in a Mixed Novell OES Server Environment 3-17
How to Get Started with NRM on OES NetWare 3-21
How to Get Started with NRM on OES Linux 3-32
How to Configure Groups and Group Operations 3-48
Exercise **3-2** Monitor the Status of Your OES Servers with Novell Remote Manager (NRM) 3-58

Objective 3 Monitor eDirectory Trees on OES with Novell iMonitor 3-59

Novell OES iMonitor Features 3-60
System Requirements 3-61
How to Access iMonitor 3-62
Novell Remote Manager Integration 3-64
Exercise **3-3** Check the Status of Your eDirectory Trees with iMonitor 3-66

Objective 4 Manage Novell OES Servers with Novell iManager. 3-67

What's New in Version 2.5 3-67
How to Access iManager 3-68
How to Initially Configure RBS 3-72
How to Configure RBS Roles 3-73
Exercise **3-4** Configure Role-Based Services. 3-76
How to Customize Novell iManager 3-77

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Exercise **3-5** Customize Novell iManager 3-85
How to Monitor Server Health 3-86
Exercise **3-6** Check the Health of Your OES Servers 3-99

Summary 3-100

SECTION 4 Implement DNS/DHCP on a Novell OES Linux Server

Objectives 4-1

Introduction 4-2

Objective 1 Configure DNS on a Novell OES Linux 4-3
How DNS Is Implemented on OES Linux 4-3
How to Configure DNS on OES Linux with YaST 4-4
What the DNS Server Configuration Files Are 4-8
How to Test DNS on OES Linux 4-11
Exercise **4-1** Configure DNS on the DA1 Linux Server with YaST 4-12

Objective 2 Configure a DHCP Server on a Novell OES Linux. 4-13
How to Configure DHCP on OES Linux with YaST 4-13
Understand the DHCP Configuration File 4-15
Exercise **4-2** Configure DHCP on the DA1 Linux Server with YaST 4-16

Summary 4-17

SECTION 5 Migrate NSS Volumes to an OES Linux Server

Objectives 5-1

Introduction 5-2
NSS Migration (NetWare to OES Linux) Requirements 5-2
The NSS Migration Scenario 5-2

Objective 1 Configure Time Synchronization on Novell OES 5-4
Identify Network Time Protocol Basics 5-4
Configure NTP on Your Network 5-11

Objective 2 Configure eDirectory with ndsconfig 5-16

 Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 3 Configure eDirectory Users to Access an OES Linux Server . 5-20
LUM Fundamentals 5-20
How to Implement LUM 5-26
How to Enable eDirectory Users for Linux Access 5-28
Exercise **5-1** Migrate the DA1 Linux Server to the DA-CORP Tree. 5-30

Objective 4 Describe Novell OES Storage Solutions 5-31
File System Support in Novell OES 5-31
NetWare Core Protocol Support (Novell Client Support) on Linux 5-32
Storage Options 5-33
OES File Storage Planning 5-34

Objective 5 Provide File Access with NCP Server 5-37
Purpose of NCP 5-38
How to Install and Configure NetWare NCP Server 5-38
How to Install and Configure Linux NCP Server 5-39

Objective 6 Configure Novell Storage Services 5-44
What NSS Is 5-44
NSS Benefits 5-45
NSS Pools and Volumes 5-47
Comparison of NSS on NetWare and NSS on Linux 5-50
NSS and EVMS on OES Linux 5-52
How to Install NSS on an OES Linux Server 5-53
How to Use the NSSMU Management Utility in OES Linux 5-54
How to Assign File System Rights for NSS Volumes on OES Linux 5-57
Exercise **5-2** Install and Configure NSS on the DA1 Linux Server 5-61

Objective 7 Migrate NSS Volumes Using the Server Consolidation Utility 5-62
Meet System and Software Requirements 5-62
Understand NetWare-to-Linux Data Migration Issues 5-63
Prepare the Source and Destination Servers 5-67
Create and Run a Consolidation Project 5-68

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise **5-3** Migrate the DATA Volume from the DA2 NetWare Server to the DA1 Linux Server 5-88

Summary 5-89

SECTION 6 Access Data on an OES Linux Server Using CIFS/Samba

Objectives 6-1

Introduction 6-2

Objective 1 Describe the Purpose of Novell Samba 6-3

Samba, SMB, and CIFS 6-3

Samba Roles for Novell OES Servers 6-3

Objective 2 Describe the Purpose and Architecture of Universal Password 6-5

Why Universal Password 6-5

Universal Password Security 6-7

Universal Password Deployment Steps 6-9

Backwards Compatibility 6-15

Password Management 6-16

Objective 3 Install Novell Samba and Configure Samba Users 6-18

Objective 4 Describe the Purpose of the Novell Samba Components 6-31

Exercise **6-1** Access CIFS Shares on the DA2 NetWare Server 6-34

Exercise **6-2** Access Samba Shares on the DA1 Linux Server. 6-35

Summary 6-36

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

SECTION 7 Migrate the iPrint Service to an OES Linux Server

Objectives 7-1

Introduction 7-2

Objective 1 Describe the Purpose and Architecture of iPrint 7-3

- What iPrint Is 7-3
- iPrint Components on Linux 7-5
- iPrint Components on NetWare 7-10
- iPrint Port Usage 7-12

Objective 2 Set Up and Manage the iPrint Server on OES Linux. 7-13

- Set Up the iPrint Server on OES Linux 7-13
- Manage the Print Manager 7-19
- Manage Printers 7-22
- Manage the Driver Store 7-29

Objective 3 Install and Configure the iPrint Client. 7-31

- Install the iPrint Client on Linux 7-31
- Install the iPrint Client on Windows 7-36
- Configure the iPrint Client Settings 7-42

Objective 4 Migrate iPrint on NetWare to OES Linux 7-46

- Migration Guidelines 7-46
- Migration Requirements 7-47
- How to Migrate iPrint Print Managers and Printer Agents Using the Server Consolidation Utility 7-48
- Post Migration Tasks 7-54
- Exercise **7-1** Migrate iPrint from the DA2 NetWare Server to the DA1 Linux Server 7-56

Summary 7-57

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

SECTION 8 Install and Configure iFolder on an OES Linux Server

Objectives 8-1

Introduction 8-2

Objective 1 Describe the Purpose and Architecture of iFolder 3.*x* 8-3

- Benefits of iFolder for the Enterprise 8-3
- Benefits of iFolder for Users 8-6
- Enterprise Server Sharing 8-8
- How iFolder 3.*x* Works 8-10
- Key Components of iFolder 8-11

Objective 2 Plan for an iFolder Services Installation 8-16

- Security Considerations 8-16
- Server Workload Considerations 8-16
- Naming Conventions for Usernames and Passwords 8-18
- Admin User Considerations 8-20
- iFolder User Account Considerations 8-23
- iFolders Data and Synchronization Considerations 8-26
- Management Tools 8-29

Objective 3 Install Novell iFolder 3.*x* and iFolder Web Access 8-32

- Prerequisites and Installation Guidelines 8-32
- How to Install iFolder on an Existing OES Linux Server . . . 8-40
- How to Configure the iFolder Enterprise Server 8-43
- How to Configure the iFolder Web Access Server 8-49
- How to Install the Novell iFolder 3 Plug-In for iManager . . 8-51
- How to Access iManager and the Novell iFolder 3 Plug-In . 8-55
- How to Provision Users and iFolder Services 8-57
- Exercise **8-1** Install and Configure iFolder 3.2 on the DA1 Linux Server. 8-63

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 4 Manage iFolder 3.*x* as an Administrator 8-64
Distribute and Install the iFolder Client 8-64
Start, Stop, and Restart the iFolder Services 8-73
Manage the Simias Log and Simias Access Log 8-74
Recover Individual Files or Directories 8-75
Configure System Policies 8-77
Modify the iFolder LDAP Settings 8-83
Manage the iFolder Web Access Server 8-89
Configure iFolder Users 8-92
Manage iFolders 8-101

Objective 5 Manage iFolder 3.*x* as a User. 8-111
Manage iFolder Accounts and Preferences 8-111
Manage iFolders 8-125
Use Novell iFolder 3.*x* Web Access 8-140
Exercise **8-2** Use iFolder 3.x on the Windows XP Professional and SLED 10 Workstations 8-144

Summary 8-145

SECTION 9 Configure White Pages (eGuide)

Objectives 9-1

Introduction 9-2

Objective 1 Describe the Purpose and Architecture of eGuide. 9-3
What eGuide Provides 9-3
eGuide System Requirements 9-5
How eGuide Works 9-6
How to Access the eGuide Client 9-8

Objective 2 Perform Basic eGuide Administration Tasks 9-10
How to Access the eGuide Administration Utility 9-10
How to Modify Search Categories 9-12
How to Configure the eGuide Display 9-16
How to Configure Security Restrictions 9-19
How to Enable Display of Organizational Charts for eDirectory Users 9-21

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise **9-1** Configure and Use eGuide on the DA1 Linux Server 9-23

Summary 9-24

SECTION 10 Provide File Access with NetStorage

Objectives 10-1

Introduction 10-2

Objective 1 Describe the Purpose and Architecture of NetStorage 10-3

What NetStorage Provides 10-4
NetStorage System Requirements 10-6
Novell NetStorage on OES Linux 10-7
Novell NetStorage on OES NetWare 10-9
How NetStorage Works 10-11
What Users See When They Access NetStorage 10-12

Objective 2 Implement and Manage NetStorage. 10-15

How to Access the NetStorage Home Page 10-15
How to Administer NetStorage from Novell iManager 10-17
How to Create Storage Location Objects and Lists 10-20
How to View or Modify Directory and File Attributes and Rights 10-25
How to Set Directory Quotas on NSS Volumes and Directories 10-27
How to Purge and Salvage Deleted NSS Files 10-28
NetStorage Implementation Guidelines 10-29
Exercise **10-1** Configure and Use NetStorage 10-34

Summary 10-35

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

SECTION 11 Plan a Novell OES Implementation

Objectives 11-1
Introduction 11-2
Objective 1 Review the Services Included in Novell OES 11-3
Objective 2 Decide Which OES Platform Is Best Suited to Provide These Services 11-7
Platform Strengths 11-7
Service Differences on the OES Platforms 11-8
Objective 3 Plan for eDirectory 11-15
Objective 4 Plan for File Services 11-17
Objective 5 Plan for Print Services 11-21
Objective 6 Plan for NetWork Server Usage 11-22
Identify a Purpose for Each Server 11-22
Review Server Requirements 11-22
Consider Coexistence and Migration Issues 11-23
Objective 7 Decide on an Installation Option Before You Start 11-24
Installation from CDs or from the Network 11-24
Pattern Deployments 11-25
Installing NSS on a Single-Drive Server 11-28
Summary 11-29

APPENDIX A eDirectory Fundamentals

Purpose and Function of a Directory A-2
What Is a Directory? A-2
Describe the Purpose of a Directory A-3
Identify Common Directory Service Uses A-4
Identify Key Components of a Basic Directory A-5
Directory System Agent (DSA) A-8

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The Role and Benefits of eDirectory A-10
The Role of eDirectory A-10
The History of eDirectory A-11
The eDirectory Database A-13
eDirectory Application Support A-14
eDirectory Components A-16
Tree A-16
Schema A-16
Objects A-17
Properties A-18
Values A-18
Object Example A-18
eDirectory Object Classes A-20
Tree Object A-21
Container Objects A-22
Leaf Objects A-27
eDirectory Object Context and Naming Conventions A-34
What Context Is A-34
Object Naming Conventions A-36
Components of a Solid eDirectory Foundation A-44
The eDirectory Foundation Model A-44
eDirectory Network Configuration Recommendations A-45

Index

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

SECTION 7 Migrate the iPrint Service to an OES Linux Server

In this section, you learn how to migrate iPrint from a NetWare 6.5 server to an OES Linux server.

Objectives

1. Describe the Purpose and Architecture of iPrint
2. Set Up and Manage the iPrint Server on OES Linux
3. Install and Configure the iPrint Client
4. Migrate iPrint on NetWare to OES Linux

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Introduction

Novell OES provides several end user services that have proven invaluable to enterprises and education.

In this section, you learn some basic administrative information about the iPrint service, and you learn how to migrate an existing iPrint service on a NetWare 6.5 server to an OES Linux server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective 1 Describe the Purpose and Architecture of iPrint

To describe the purpose and architecture of iPrint, you need to know the following:

- What iPrint Is
- iPrint Components on Linux
- iPrint Components on NetWare
- iPrint Port Usage

What iPrint Is

iPrint lets mobile employees, business partners, and customers access printers from a variety of remote locations using existing Internet connections.

Whether users are working in an office building, telecommuting from home, or attending a sales meeting in another country, iPrint ensures that they can print documents quickly, easily, and reliably.

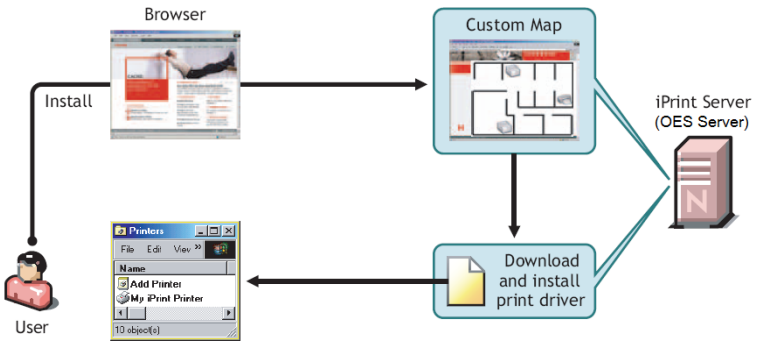
Using a web browser, users point to a web page that displays the printers available for installation.

When the user selects a printer, the iPrint client is installed (if not installed previously), the printer's driver is downloaded, and a printer is created on the user's workstation, enabling the user to send documents to the printer from any application on the desktop

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The following illustrates this process:

Figure 7-1



Using iPrint, mobile users no longer need to contact a busy network administrator to find out a printer's name and context, and the required printer driver.

Instead, mobile users work within a familiar web browser to locate nearby printers using iPrint's Printer List web page or maps created by the administrator.

Companies can also lower communication costs by reducing the need to fax documents between offices; instead, companies can use their existing Internet connections to print documents to remote printers.

iPrint uses the Internet Printing Protocol (IPP), an industry standard, to eliminate the complexities of printing over the Internet and to make location-based printing a reality.

The benefits of IPP include the following:

- Uses the IP protocol
- Provides broad vendor support
- Works over local networks and the Internet
- Provides for print data encryption (SSL, TLS)
- Provides a standard print protocol for all platforms (such as Linux, Macintosh, and Windows)

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.



For more information about IPP, see the documents available on the Printer Working Group web site at http://www.pwg.org/ipp/index.html.

In addition to the benefits of IPP, Novell's implementation of iPrint adds the following value:

- Printer driver download and installation
- Location-based printing
- Browser-enabled printer installation interface
- Customizable user interface
- Secure information transfer

For secure printing needs, iPrint integrates with Novell eDirectory to ensure that only authorized users can access the printer.

Users are required to authenticate with their eDirectory username and password. Print data is also encrypted to ensure that sensitive print data is kept secure and unaltered.

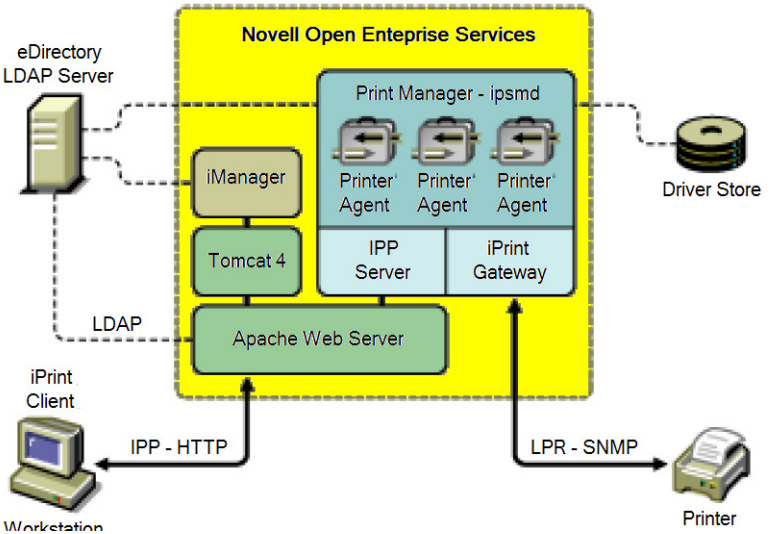
iPrint Components on Linux

iPrint on an OES Linux server consists of three main components: the Print Manager, the Driver Store, and the iPrint Client.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Other supporting components include Apache Web Server, Novell iManager, and eDirectory:

Figure 7-2



The following describes each iPrint component:

- Print Manager
- Driver Store
- iPrint Client
- Apache Web Server
- Novell iManager

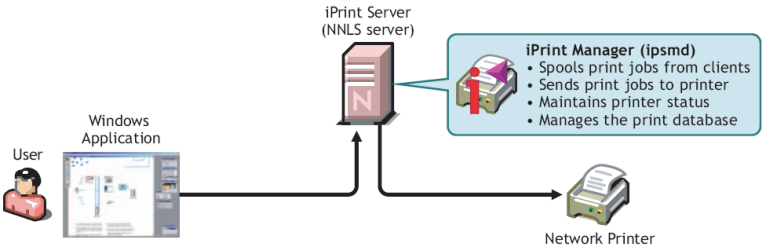
Print Manager

The Print Manager is an object in the eDirectory tree as well as software that runs on an OES server. The Print Manager provides a platform for Printer Agents to reside on the server. Printer

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Agents are representations of actual printers. Print jobs are submitted to the Print Manager; the print job is then forwarded to a printer when the printer is ready:

Figure 7-3



A single Print Manager can handle print jobs for multiple printers.

Depending on your network configuration (for example, remote locations), you can create additional Print Managers on other servers, but only one Print Manager can exist on any one server.

The Print Manager uses the following access control components to authorize users to print:

- **Printer Agent.** The Printer Agent is an entry in the Print Manager database that represents the physical printer.

 When you create a printer, a Printer Agent is created in the Print Manager's database and a Printer object is added to eDirectory.

 The Printer Agent manages the processing of print jobs, answers queries from network clients about a print job or attributes of a printer, and provides SNMP (Simple Network Management Protocol) information that is displayed in the Print Manager Health Monitor.

- **IPP server.** The IPP server's main function is to handle IPP requests from the web server and deliver the requests to the Print Manager (Linux) or to the Broker (NetWare).

- **iPrint gateway.** The gateway maintains communication with the printers. When a printer is ready, the gateway requests print jobs from the Print Manager for the printer.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The print jobs are sent to the printer using LPR over the TCP/IP protocol. Using SNMP, the gateway also queries printers to get their status and other printer information.

Driver Store

The Driver Store is an eDirectory object. Only one Driver Store is required on a network but, depending on your network configuration, you can create additional Driver Stores.

The fewer Driver Stores running, the better because you do not need to track which Driver Store has which printer drivers.

The Driver Store is a repository of printer drivers for your print system.

When the first user of a printer installs that printer, the Print Manager requests the associated printer driver from the Driver Store, and the Print Manager saves the printer driver to disk for future use.

Periodically, Print Managers refresh their saved copies of printer drivers for the printers they are hosting with updated printer drivers from their associated Driver Store.

iPrint Client

The following iPrint clients are available:

- Linux iPrint Client
- Macintosh iPrint Client
- Windows iPrint Client

Linux iPrint Client

The Linux iPrint client lets Linux workstations install iPrint clients and includes the following components:

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Browser plug-in.** The iPrint client contains a browser plug-in for Mozilla-based browsers.

 This plug-in lets you install printers through your web browser.

- **Console utility.** The Linux iPrint client includes the iprntcmd utility, which lets you install printers, print test pages, and upload drivers to a Driver Store from a console prompt.

- **CUPS Integrator.** The client integrates with the CUPS back end and uses the CUPS local spooler to send print jobs to the Print Manager.

Macintosh iPrint Client

The Macintosh iPrint client contains a browser plug-in for the Safari web browser, which lets you install printers through your web browser.

The client integrates with the CUPS back end and uses the CUPS local spooler to send print jobs to the Print Manager.

Windows iPrint Client

The Windows iPrint client lets you install iPrint printers and configure iPrint on your workstation, and it includes the following components:

- **Print Provider.** The iPrint Print Provider communicates directly with the Windows Spooler, which takes print jobs from applications and delivers them to a print provider.

 Upon startup, the iPrint client ensures that the iPrint Print Provider is first in the list of providers.

 When a print job is destined for an iPrint printer, the iPrint Print Provider delivers the print job to the Print Manager.

- **Browser plug-in.** The iPrint client contains a browser plug-in for Mozilla-based browsers and Internet Explorer. The Internet Explorer plug-in is an OCX-based plug-in that lets you install printers through your Web browser.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

- **Client configuration.** Through the iPrint client configuration screen, you can take advantage of several advanced client features.
- **Command line utilities.** The iPrint MS-DOS commands let you install iPrint printers without a web browser and capture LPT ports to iPrint printers.

 These commands are useful when you have legacy applications that require output to an LPT port, or when you want to add printers through a login script.

Apache Web Server

Apache 2.0 is the Web server for iPrint. The Web server serves up HTML pages, handles secure (SSL/TLS) and nonsecure requests, and utilizes LDAP for authentication.

Novell iManager

You use Novell iManager to create, configure, and manage your iPrint system.

For complete management, including uploading printer drivers and PPD files, you need to access iManager from a workstation with the iPrint client installed.

iPrint Components on NetWare

Novell iPrint on NetWare uses the NDPS (Novell Distributed Print Services) infrastructure.

In addition to NDPS, iPrint uses the following components on NetWare:

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Print broker (NetWare).** This repository stores the drivers on an OES NetWare server for your network printers. It is the first component you configure and is represented by an object that you create in eDirectory.
- **Printer drivers.** These platform-specific printer drivers and PostScript Printer Description (PPD) files are stored in the Broker and are installed on workstations when users select a target printer.

 Printer drivers and PPD files exist as file structures with the Driver Store and broker and are not represented by objects in eDirectory.
- **Printer objects.** These eDirectory objects, which you create, store information about the printers available through iPrint.

 The information stored in a Printer object is used each time its associated printer is added to a workstation's list of available printers.
- **Print manager.** This is an eDirectory object. On an OES NetWare server, it is an NLM (ippsrvr.nlm).

 Print manager receives print jobs from users and forwards them to the target printer when it is ready. It is represented by and controlled through an eDirectory object that you configure.

 When an eDirectory Printer object is configured as an iPrint printer, the Print Manager automatically loads this NLM on the server, which then generates a URL for the printer.
- **iPrint client.** This set of browser plug-ins is automatically installed the first time it interacts with iPrint. The iPrint client can be used on both Macintosh and Windows workstations; the Novell client is not required.
- **HTML pages.** These are used to install the iPrint client software and printers as well as to view and manage print jobs. These pages are customizable.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

iPrint Port Usage

iPrint can use any port specified on Apache; however, iPrint defaults to two primary ports:

- **Port 443.** All secure printing occurs over port 443 using SSL.
- **Port 631.** All non-secure printing occurs over port 631.

 The iPrint client also supports TLS. If your system, including the client, is configured to use TLS, all secure and non-secure printing occurs over port 631.

 During OES installation of the iPrint software, the CUPS back-end components are disabled on the server to avoid port 631 conflicts.

 Because iPrint uses CUPS to render print jobs before sending the print job to the Print Manager, printing from the server itself using CUPS or iPrint is not available.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 2 Set Up and Manage the iPrint Server on OES Linux

To set up and manage iPrint on an OES Linux server, you need to know how to do the following:

- Set Up the iPrint Server on OES Linux
- Manage the Print Manager
- Manage Printers
- Manage the Driver Store

Set Up the iPrint Server on OES Linux

If you select iPrint during a Novell OES Linux server installation (the default setting), the iPrint software components are automatically installed on your OES Linux server.

To set up the iPrint server, you need to do the following:

- Create a Driver Store
- Add Printer Drivers
- Create a DNS Name for the Print Manager
- Create a Print Manager
- Create a Printer

Create a Driver Store

You need only one Driver Store for your print system; however, depending on your network setup, you can add additional Driver Stores. You need to create a Driver Store to create a Print Manager.

The following are general steps for creating a Driver Store:

1. From iManager (on the left), select **iPrint > Create Driver Store**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. Fill in the appropriate fields.

 For explanations about the fields, select **Help**.

3. When you finish filling in the fields, select **OK**.

After the Driver Store is created, and the daemon is loaded on the server, you can start uploading printer drivers.

Add Printer Drivers

A printer driver or PostScript Printer Description (PPD) file is a software entity that directly supports a physical printer, enabling it to carry out its functions.

Hardware vendors develop printer drivers and PPD files, that are specific to each printer. Most printers require different printer drivers for each operating system they interact with.

You can view a list of the printer drivers and PPD files you have uploaded to the Driver Store using iManager. You can add printer drivers and PPD files from diskettes, CDs, and the workstation operating system.

The Driver Store daemon must be running to add resources, and the iPrint client must be installed on a Linux or Windows workstation.

To add printer resources to the Driver Store, do the following:

1. From Novell iManager (on the left), select **iPrint > Manage Driver Store**; then browse to and select the ***Driver Store*** you want.
2. Select **Drivers**; then select the ***client platform*** you want to work with.
3. Do one of the following:
 - Add printer resources from a printer driver .inf file or PPD file by selecting **Add from File**.

 or

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Add drivers from the workstation you are running iManager from by selecting **Add from System**.

 The drivers installed on your workstation are made available for upload to the Driver Store.

 You can upload only drivers for the same platform as the workstation.

4. Select the ***driver*** you want; then select **OK**.
5. Save your changes by selecting **OK**.



You can also install driver files from a Linux console prompt using the iprntcmd command.

For details, see "Using iprntcmd on Linux and Macintosh," on page 37 in the *Novell OES iPrint Administration Guide for Linux*.

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Create a DNS Name for the Print Manager

The Print Manager creates a URL for each printer based on the Print Manager configuration.

When you create the Print Manager, you can specify an IP address or DNS name for the iPrint Service.

You should always use a DNS name because using an IP address forces users to delete and reinstall printers if the IP address changes.

To create a DNS name (record) for the Print Manager from OES Linux, do the following:

1. From the OES Linux KDE desktop, select the **YaST** icon.

 A Run as root - KDE su dialog appears.

2. Enter the root ***password***; then select **OK**.

 The YaST Control Center appears.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

3. From the left, select **Network Services**; from the right, select **DNS Server**.

 A DNS Server - Start-Up configuration page appears.

4. From the left, select **DNS Zones**.

 A DNS Server - DNS Zones page appears.

5. From the list, make sure that the ***zone*** you want associated with the Print Manager is selected; then select **Edit Zone**.

 The Zone Editor page appears.

6. Select the **Records** tab.

7. Create a record for the IP address associated with the Print Manager (normally the OES Linux server IP address) by entering the following:

 - **Record Key.** The DNS name you want associated with the Printer Manager.
 - **Type.** The record type (normally an A record).
 - **Value.** The IP address associated with the Print Manager.

8. When you finish, select **Add**; then continue by selecting **OK**.

 You are returned to the DNS Server - DNS Zones page.

9. From the list, select the reverse lookup zone (in-addr.arpa) for the Print Manager; then select **Edit Zone**.

 The Zone Editor page appears.

10. Select the **Records** tab.

11. Create a reverse-lookup record for the Print Manager DNS name by entering the following:

 - **Record Key.** The reverse of the IP address associated with the Print Manager.

 For example, if you have associated 10.200.200.2 with the Print Manager, you need to enter **2.200.200**.

 - **Type.** The record type (normally a PTR record).
 - **Value.** The full DNS name (including zone) of the Print Manager.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

12. When you finish, select **Add**; then continue by selecting **OK**.

 You are returned to the DNS Server - DNS Zones page.

13. Select **Finish**.

 After the configuration is complete, you are returned to the YaST Control Center.

If you are currently running the Print Manager on a NetWare server, you also need to configure the Print Manager on the NetWare server to use the DNS name.

Do the following:

1. From the NetWare server, press **Ctrl+Esc**; then display the system console by entering **1**.
2. From the system console command prompt, unload the Print Manager by entering the following:

 unload ndpsm

 A message appears indicating that the Print Manager has been unloaded.

3. Load the Printer Manager by entering the following (all on one line):

 ndpsm *.printmgr.example.novell/*
 dnsname=*printmanager.example.com*

 where ***.printmgr.example.novell*** represents the full DN (distinguished name) of the Print Manager object in the eDirectory tree, and ***printmanager.example.com*** represents the full DNS name of the Print Manager.

 The /dnsname switch lets you configure the Print Manager to use a DNS name instead of an IP address.

 You only need to use this switch once; after that, the Print Services Manager remembers the DNS name.

 The Printer Agent List appears with the HP-DJ printer listed.

4. Display the Current Screens menu by pressing **Ctrl+Esc**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

You have finished configuring the Print Manager.

Create a Print Manager

You need to create at least one Print Manager for your print system; however, depending on your network setup, you can create additional Print Managers (for example, across a WAN link).

The Print Manager must be running in order to create printers.



The Print Manager creates a URL for each printer based on the Print Manager configuration.

When you create the Print Manager, you can specify an IP address or DNS name for the iPrint service.

You should always use a DNS name because using an IP address forces users to delete and reinstall printers if the IP address changes.

A Driver Store must exist before you create a Print Manager.

To create a Print Manager, do the following:

1. Make sure you have configured a DNS name for the Print Manager
2. From iManager (on the left), select **iPrint > Create Print Manager**.
3. Fill in the appropriate fields.

 To view explanations about the fields, select **Help**.
4. Make sure the **Start Print Manager after Creation** checkbox is selected.



If you do not select this option, you have to start the Print Manager by using **Manage Print Manager > Manager Control** in iManager or by entering **/etc/init.d./novell-ipsmd start** at a shell prompt.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

5. When you finish, select **OK**.

 After the Driver Store is created and the daemon is loaded on the server, you can start adding printer drivers.

Create a Printer

After you have created a Print Manager, you can create a printer by doing the following:

1. From iManager (on the left), select **iPrint > Create Printer**.
2. Follow the prompts and fill in the fields.

 You can view explanations about the fields by selecting **Help**.
3. When you finish, select **Next**; then select the drivers for this printer.



If the printer drivers for this printer are not listed, you can still create the printer.

After the printer is created, add the printer drivers to the Driver Store, and then associate the drivers to the printer by selecting **Manage Printer > Drivers**.

4. When you finish, create the printer by selecting **Next**.

Manage the Print Manager

The Print Manager uses a database to store information about the printers it controls. The database creates a backup every night at midnight and when you create or delete a printer.

The last four backups are saved. When a new backup file is created, the oldest of the four stored files is deleted. If the oldest backup file is older than four days, then the Print Manager creates a new backup.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If the database fails to load through normal mechanisms, you can use the backup database by doing the following:

1. Rename /var/opt/novell/iprint/psmdb.* to psmdbold.*.
2. Rename /var/opt/novell/iprint/psmdbsav.* to psmdb.*.
3. Start the Print Manager.

When you create a Print Manager, a configuration file is created in /etc/opt/novell/iprint. The file name is *print_manager_name*.ipsmd.conf.

A separate file is created for each Print Manager that is created and assigned to run on the same server. Only one Print Manager can run on the server at a time.

For information about the entries in the configuration file, see /etc/opt/novell/iprint/ipsmd-template.conf.

The ipsmd.conf file links to the configuration file of the currently loaded Print Manager. To load a different Print Manager on the server, use iManager.

If you attempt to load a Print Manager when one is already running, you will receive an error message instructing you to unload the current Print Manager before loading the new one.

If you need to change the eDirectory server assignment for the Print Manager or Driver Store, edit the DSServer1=*entry* in the corresponding configuration file (*print_manager_name*_ipsmd.conf or idsd.conf) located in /etc/opt/novell/ iprint/.

You can start and stop the Print Manager in one of the following ways:

- **From the command line.** The Print Manager uses init scripts for starting and stopping the daemon.

 To load the Print Manager from the command line, enter the following:

 /etc/init.d/novell-ipsmd start

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You can also use the actions stop, reload, force-reload, and status.

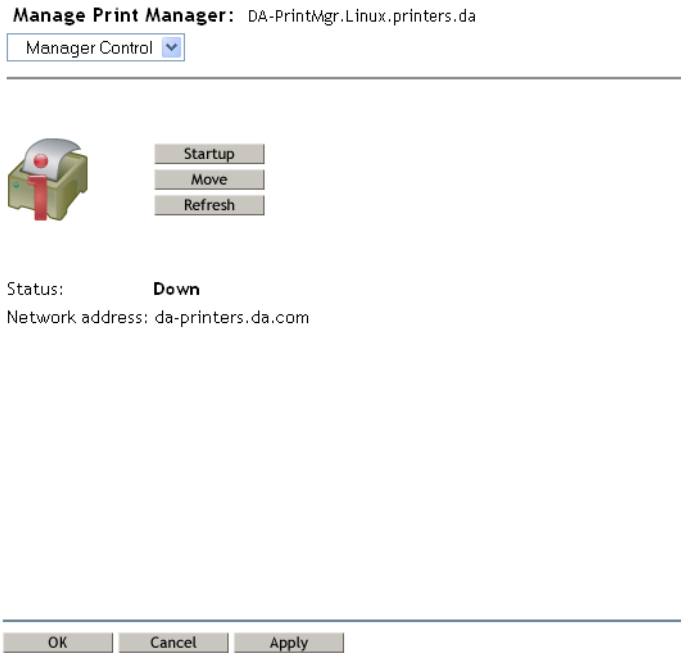
- **From iManager.** On the Manager Control Property page, you can view the Print Manager's status and unload or load the Print Manager daemon.

 Do the following:

 1. From Novell iManager, select **iPrint > Manage Print Manager**.
 2. Browse to and select the Print Manager you want to manage.

 The following appears:

Figure 7-4



 3. Stop the Print Manager by selecting **Manager Control > Shutdown**.
 4. Select **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Manage Printers

Although the default settings let users print without additional configuration, you might want to modify some of those settings so that you can manage your printing resources more effectively.

You can modify the settings by doing the following:

- Create Additional Printers
- Manage Printer Agents
- Use Printer Driver Profiles
- Enable iPrint Direct
- Manage Print Jobs

Create Additional Printers

Before creating additional printers, ensure you meet the following prerequisites:

- Have the Supervisor right to the destination container where its associated Printer object is to reside.
- Be designated as a manager of the Print Manager that controls this printer.
- Have a Driver Store running.
- Have a Print Manager running.

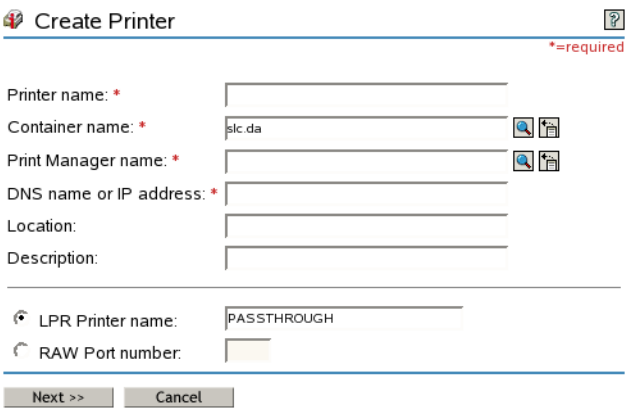
To create additional printers, do the following:

1. From Novell iManager, select **iPrint > Create Printer**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 7-5



2. Fill in the fields.

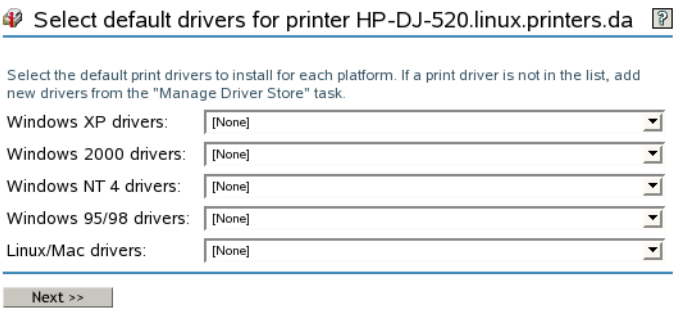
 Select Help for explanations about the fields.

3. Select **OK**.

4. Select **Next**.

 The following appears:

Figure 7-6



5. Select the ***drivers*** for this printer.

 If the printer drivers for this printer are not listed, you can still create the printer.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

After the printer is created, you can add the printer drivers to the Driver Store and then associate the drivers to the printer by selecting Manage Printer > Drivers.

These drivers are automatically downloaded to users' workstations when they install the printer in the future.

Because the list of printer drivers included with this product is limited, you can add drivers to the Driver Store.

If you do not select a driver, users are prompted to provide a disk with the appropriate driver the first time they install this printer on their workstations.

6. Create the printer by selecting **Next**.

Manage Printer Agents

Using iManager, you can manage Printer Agents.

You can start up and shut down a Printer Agent, pause and resume input and output, view printer information, set configuration settings, and change the printer drivers.

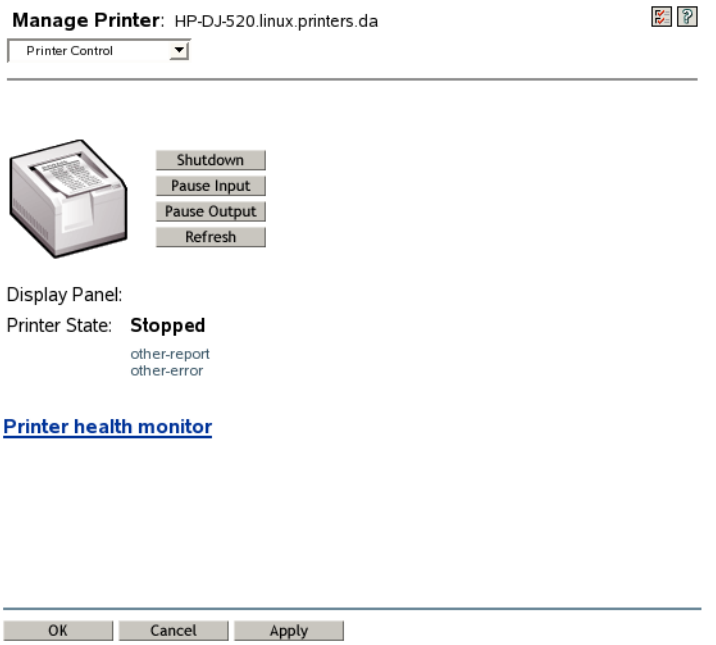
Do the following:

1. From Novell iManager, select **iPrint > Manage Printer**.
2. Browse to and select the ***printer*** you want to manage.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 7-7



3. Use the tabbed property pages (or drop-down list in Firefox) to complete the appropriate task.

Use Printer Driver Profiles

Printer driver profiles let you set the driver defaults for a Windows printer driver. Then you associate the printer driver profile to a printer so that when the printer is installed, it is configured with the settings you want.

For example, in a law office you might want the default paper size to be legal size. This means every time the printer and corresponding driver are installed on a workstation, the paper size is set to legal size.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

To use printer driver profiles, you need to know how to do the following:

- Create, Modify, and Delete a Printer Driver Profile
- Associate a Printer Driver Profile with a Printer

Create, Modify, and Delete a Printer Driver Profile

When creating a printer driver profile, you work directly with a platform-specific printer driver. For this reason, you need to create and modify profiles from the same operating system platform as the printer driver.

For example, to create or modify a Windows 2000 printer driver profile, you must access iManager and complete the task from a Windows 2000 workstation.

Do the following:

1. From Novell iManager, select **iPrint > Printer Driver Profile**.
2. Browse to and select the ***Print Manager*** where you want the driver profile stored and made available to the printers on that manager.
3. Select one of the following:
 - **Create Printer Driver Profile.** Creates a new printer driver profile.
 - **Delete Printer Driver Profile.** Deletes an existing driver profile.
 - **Modify Printer Driver Profile.** Changes the settings of an existing printer driver profile.
4. Select **OK**.

Associate a Printer Driver Profile with a Printer

After creating a printer driver profile, you need to associate it with a printer. Do the following:

1. From Novell iManager, select **iPrint > Manage Printer**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. Browse to and select the ***printer*** you want to modify.
3. Select **Drivers >** ***printer_driver_operating_system***.
4. From the list of Available Drivers, select the ***printer driver***.
5. From the list of Available Driver Profiles for Selected Driver, select the ***profile*** you want associated with this printer.

 If you do not want a profile associated, select None.
6. Save the changes by selecting **OK**.

Enable iPrint Direct

Users of an iPrint Direct-enabled printer send print jobs directly to the printer instead of sending jobs to the Print Manager first.

The job is sent to the printer in LPR or raw 9100 format, depending on the setting gateway autoload command for the printer.

Although this greatly reduces server communication, the ability to audit print jobs is lost. iPrint Direct still supports driver updates, and printer information is gathered directly from the printer using SNMP.

Do the following:

1. From Novell iManager, select **iPrint > Manage Printer**.
2. Browse to and select the ***printer*** you want to enable iPrint Direct printing for.
3. Select **Client Support > iPrint Direct**.
4. Select the **Enable iPrint Direct Printing** option.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Manage Print Jobs

The following provides information about the print job management features of iPrint:

- View Print Job Information
- Delete Print Jobs
- Change the Order of Print Jobs

Users designated as managers or operators for a printer can perform these tasks for all jobs routed to that printer; individual job owners can perform these tasks only for their own print jobs.

View Print Job Information

You can view information about individual print jobs waiting to be processed by a specific printer by doing the following:

1. From Novell iManager, select **iPrint > Manage Printer**.
2. Browse to and select the ***printer*** the job was sent to.
3. Select **Printer Control > Jobs**.

 Information about print jobs is displayed.

Delete Print Jobs

Administrators can delete any print job after it has been submitted if the job has not yet started printing. Users can delete only their own print jobs.

Do the following:

1. From Novell iManager, select **iPrint > Manage Printer**.
2. Browse to and select the ***printer*** the job was sent to.
3. Select **Printer Control > Jobs**.
4. Select the ***check box*** next to the job you want to delete.
5. Select **Delete**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Change the Order of Print Jobs

Occasionally, you might need to print a job ahead of other jobs that have already been submitted to a printer but have not yet started printing.

Administrators, managers, and operators can move any job up or down the list. Users can move only their own jobs and can only move them down the list.

Do the following:

1. From Novell iManager, select **iPrint > Manage Printer**.
2. Browse to and select the ***printer*** the job was sent to.
3. Select **Printer Control > Jobs**.
4. Select the ***check box*** next to the job you want to modify.
5. Move a print job up the list by selecting **Promote**.

Manage the Driver Store

When you create a Driver Store, a configuration file is created in /etc/opt/novell/iprint. The file name is idsd.conf.

Each time you create a Driver Store object using iManager and assign it to the same server, a separate entry is added to idsd.conf.

Although you can have several Driver Stores assigned to a server, all printer driver files are stored in one file structure on the server.

For information about the entries in the configuration file, see /etc/opt/novell/iprint/idsd.conf.

If you need to change the eDirectory server assignment for the Print Manager or Driver Store, edit the DSServer1=*entry* in the corresponding configuration file (*print_manager_name*_ipsmd.conf or idsd.conf) located in /etc/opt/novell/ iprint/.

You can start and stop the Driver Store in one of the following ways:

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **From the command line.** The Driver Store uses init scripts for starting and stopping the daemon.

 To load the Driver Store from the command line, enter the following:

 /etc/init.d/novell-idsd start

 You can also use the **stop**, **reload**, **force-reload**, and **status**.

- **From iManager.** On the Manager Control Property page, you can view the Print Manager's status and unload or load the Print Manager daemon.

 Do the following:

 1. From Novell iManager, select **iPrint > Manage Driver Store**.
 2. Browse to and select the ***Driver Store*** you want to manage.
 3. Stop the Driver Store process by selecting **Driver Store Control > Shutdown**.
 4. Select **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 3 Install and Configure the iPrint Client

To install and configure the iPrint client, you need to know how to do the following:

- Install the iPrint Client on Linux
- Install the iPrint Client on Windows
- Configure the iPrint Client Settings

Install the iPrint Client on Linux

For iPrint to work properly, a workstation must have the iPrint client installed.

You can distribute the client to workstations in a variety of ways, such as using the iPrint Printer List web page, using distribution software like ZENworks, or creating login scripts.

To install the iPrint client on Linux, you need to know the following:

- iPrint Client Requirements
- Access Control to the Workstation Print System
- How to Install the iPrint Client and Your First Printer on Linux

iPrint Client Requirements

For iPrint to work properly, Linux workstations need the following:

- Novell Linux Desktop or SUSE 9.2 (or later) Professional installed
- Konqueror or a Mozilla-based browser such as Epiphany, Firefox, or Galeon

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

In addition to these requirements, you need to know the following:

- To install the client, you must have the root password or rights as root.
- This release of the iPrint Linux client does not support printing to a secure printer that requires a user name and password.
- If the iPrint server is busy when your installed printer attempts to communicate, CUPS moves the printer into an error state and holds all print jobs.

 To release print jobs, use the printer management utility to restart the printer.

Access Control to the Workstation Print System

The Linux iPrint client is packaged in two different, specialized installations that control access to the workstation's print system.

The following explains the differences between the two clients:

Table 7-1

iPrint Client Filename	Description
novell-iprint-xclient-sh-0.5.20050201- 4.i586.rpm	Security high. Limited access to the print system. This client requires workstation users to be defined with lppasswd to install, delete, or administer printers on the workstation. When performing one of these print operations, the user is asked for a password. By default, the iPrint Printer List web page installs this RPM.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 7-1**

iPrint Client Filename	Description
novell-iprint-xclient-sl-0.5. 20050201- 4.i586.rpm	Security low. Unlimited access to the print system. This client allows all users of the workstation to install, delete, or administer printers and print jobs on the workstation, including printers and print jobs of other users.

These clients do not affect installation of the iPrint client or printing capabilities—just access to the workstation print system. To install the iPrint client, you still need root permissions.

To upload drivers from the system, you need to be defined with lppasswd; otherwise, when you try to add drivers from the system, the driver list will be blank.

To define a user to be part of lppasswd, you can use the following command:

lppasswd -a *linux_user_account* -g sys

How to Install the iPrint Client and Your First Printer on Linux

You can use one of the following methods to install the iPrint client on user workstations:

- Install the Client from the iPrint Printer List Web Page
- Deliver the Client Using Distribution Software

Install the Client from the iPrint Printer List Web Page

You can download and install the iPrint client from the iPrint Printer List web page that is stored on the server where the Print Manager is loaded.

By default, the link is set to install the high security novell-iprint-xclient-sh-0.5.20050201-4.i586.rpm client.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You can change this by creating a symbolic link in /var/opt/novell/htdocs using the following command:

ln -sf *client* novell-iprint-client.rpm

where ***client*** is the client filename listed in Table 7-1.

To install the iPrint client (and your first printer), do the following:

1. From a web browser on the Linux desktop, enter the following iPrint server URL:

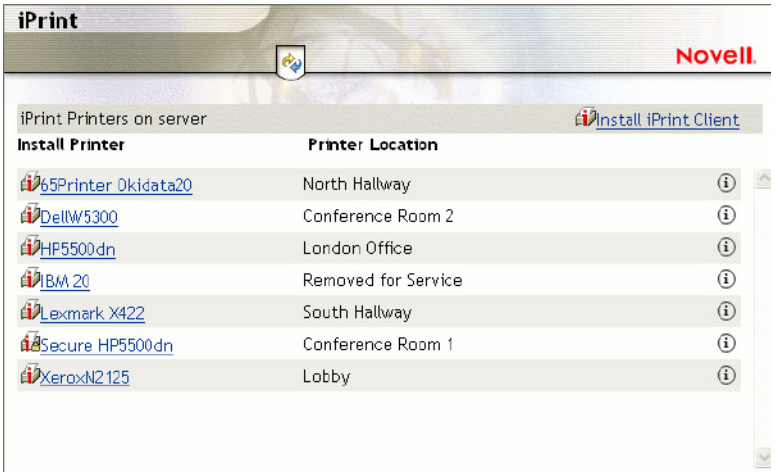
 http://*server_IP_ address_or_dns_name*/ipp

 For example, if the DNS name where the iPrint server is installed is DA3.da.com, you would enter the following:

 http://DA3.da.com/ipp

 A page similar to the following appears:

Figure 7-8



2. Select the printer you want to install.

 If the iPrint client is not yet installed on your workstation, you are prompted to install it.

3. When prompted, save the iPrint client RPM to your desktop or home directory.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

4. Install the iPrint client RPM by double-clicking the RPM.

 If a file association for the RPM does not exist, use an RPM installer program.

5. Exit and restart your web browser before installing your first printer.



If you are using the Konqueror browser, you must rescan for plug-ins by selecting **Settings > Configure Konqueror Plug-ins > Plug-Ins > Scan for New Plug-ins**. You can then restart the Konqueror browser to install a printer.

If you are using a nonstandard installation of a browser and the plug-in does not appear, create a symbolic link in the browser's plug-in directory using the following command:

ln -s /opt/novell/iprint/plugin/npnipp.so

6. Enter the iPrint server ***URL***.

7. From the iPrint server page, select a ***printer*** you want to install.

 During the printer installation, iPrint downloads and installs the printer driver, if one is associated with the printer, and installs the printer on the user's workstation.

 The first time a printer is installed, printer drivers are forced to the workstation, even if the workstation contains a newer driver.

 Print managers refresh their saved copies of printer drivers for the printers they are hosting with updated printer drivers from the associated Driver Store.

Deliver the Client Using Distribution Software

You can use client distribution software (such as ZENworks) to deliver the iPrint client and possibly printers to your client workstations.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



For more information, see the documentation for your distribution software.

Install the iPrint Client on Windows

To install the iPrint client on Windows, you need to know the following:

- iPrint Client Requirements
- iPrint Client Installation Files
- How to Distribute the iPrint Client for Windows
- How to Install a Printer

iPrint Client Requirements

The following are requirements for installing the iPrint client on a Windows system:

- Windows 95/98/ME or Windows NT/2000/XP Professional

 To install the client on Windows NT/2000/XP, you must have Administrator rights or be a Power User on Windows NT/2000.

- A web browser with JavaScript enabled and one of the following versions:
 - Microsoft Internet Explorer 5.5 or later
 - Mozilla-based Web browser

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



The iPrint Client for Windows uses ActiveX controls when using Internet Explorer. By default, Internet Explorer's Run ActiveX Controls and Plug-ins are enabled.

However, if these controls or plug-ins have been disabled, you need to reenable them for iPrint to work correctly. This setting is found in Tools > Internet Options > Intranet > Custom Level in Internet Explorer.

You need to enable the setting on the Internet page, if you are running across the Internet

iPrint Client Installation Files

The Windows iPrint client is packaged in several different, specialized installations. Depending on your distribution method or need, select the file you want.

The following compares the different types of installations:

Table 7-2

iPrint Client Filename	Description
nipp.exe	Installs the iPrint Client and displays dialog boxes and progress windows that require user intervention. This is the default installation program.
nipp.zip	A WinZip version of the client that can be used with distribution software programs. After the file is unzipped, run setupipp.exe. For a list of the command line parameters that you can use with setupipp.exe, enter setupipp.exe /h at a command prompt.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 7-2**

iPrint Client Filename	Description
nipp-s.exe	Installs the iPrint Client. A screen displays the progress of the installation, but requires no user intervention. Because Windows 9*x* users must reboot their workstations after the client is installed, you should use nipp-sr.exe unless you are using a software distribution package that reboots the workstation.
nipp-sr.exe	Installs the iPrint Client and reboots the workstation. A screen displays the progress of the installation, but no user intervention required.
nipp-su.exe	Uninstalls the iPrint Client. A screen displays the progress of the uninstall, but requires no user intervention.
nipp-u.exe	Uninstalls the iPrint Client. The user confirms the request to uninstall the client, and then a screen displays the progress of the uninstall.

Windows 9*x* users must restart their workstations. After the iPrint Client is installed, Windows NT/2000/XP users do not need to restart unless they are using iPrint utilities to capture LPT ports.

How to Distribute the iPrint Client for Windows

You can use one of the following methods to install the iPrint client for Windows on users' workstations:

- Install the Client from iPrint Printer List Web Page
- Deliver the Client Using Distribution Software

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Install the Client from iPrint Printer List Web Page

You can download and install the iPrint client from the iPrint Printer List web page that resides on the server where the Print Manager is loaded.

1. From a web browser on the Linux desktop, enter the following iPrint server URL:

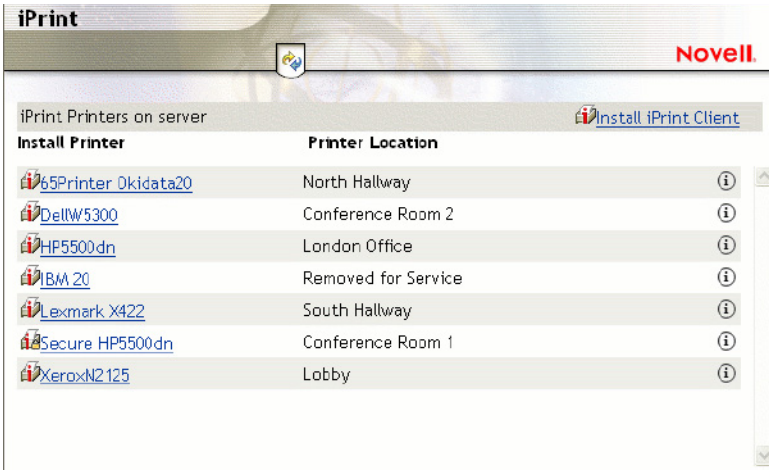
 http://*server_IP_ address_or_dns_name*/ipp

 For example, if the DNS name where the iPrint server is installed is DA3.da.com, you would enter the following:

 http://DA3.da.com/ipp

 A page similar to the following appears:

Figure 7-9



2. Select the printer you want to install.

 If the iPrint client is not yet installed on your workstation, you are prompted to install it.

3. When prompted, run the iPrint client installation file (nipp.exe).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Deliver the Client Using Distribution Software

Using client distribution software (such as ZENworks), you can also deliver the iPrint client and possibly printers to your client workstations.

For more information, see the documentation for your distribution software.

For example, when using Novell's ZENworks, you can use any of the iPrint Clients described in "iPrint Client Installation Files" on 7-37 to deliver the Windows iPrint Client.

In most cases, you will likely need to use the nipp.zip file to deliver the client to the desktop and execute setupipp.exe with one of the command line parameters.

How to Install a Printer

You can install and distribute iPrint printers in the following ways:

- Use the iPrint Printer List Web Page
- Create Location-Based Printing Web Pages

Use the iPrint Printer List Web Page

iPrint generates a list of printers associated with a Print Manager that can be used to install the iPrint client, install an iPrint printer, or check the status and configuration of a printer, including a list of print jobs.

To use the iPrint Printer List web page, do the following:

1. From a web browser on the Linux desktop, enter the following iPrint server URL:

 http://*server_IP_ address_or_dns_name*/ipp

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

For example, if the DNS name where the iPrint server is installed is DA3.da.com, you would enter the following:

http://DA3.da.com/ipp

2. (Conditional) If the iPrint client is not installed, install it when prompted.
3. From the list of available printers, select the ***printer*** you want to install and follow the prompts.

During the printer installation, iPrint downloads and installs the printer driver, if one is associated with the printer, and installs the printer on the user's workstation.

The first time a printer is installed, printer drivers are forced to the workstation, even if the workstation contains a newer driver.

Print Managers refresh their saved copies of printer drivers for the printers they are hosting with updated printer drivers from the associated Driver Store.

Create Location-Based Printing Web Pages

Location-based printing lets users select printers based on locations by using a list view or a map.

Using a list view, printer locations can be displayed using HTML pages organized by building, office location, eDirectory context, etc. You configure the lists in a way that best suits the users' needs.

For an example of using a list view, see /var/opt/novell/iprint/htdocs/examples/example2/innerweb.htm.

Using the iPrint Map Designer, you can create maps of printer locations by using drag-and-drop technology. After the maps are created, they can be posted on a Web server for users to access.

When users view the maps, they can find a printer close to their location and then click its icon. The client software (if not yet installed) and the printer are installed on their workstations.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



For information on using the iPrint Map designer, see "Creating Location-Based Maps with iPrint Map Designer" on page 49 in the *Novell OES iPrint Administration Guide for Linux*.

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Configure the iPrint Client Settings

To configure iPrint client settings, you need to know how to do the following:

- Use a Proxy Server
- Manage Passwords for Remote iPrint Servers
- Manage iPrint's System Tray Icon
- Manage Print Job Notifications

Use a Proxy Server

A proxy server sits between a client and another server that the client is trying to communicate with.

Often proxy servers are used in conjunction with a firewall to keep internal addresses private while only exposing the proxy server's address to external users.

If you are using a proxy server and have users that need to submit print jobs through a proxy server, you can use the iPrint client's Proxy setting.

The client sends all print-related requests, such as a print job, to the proxy server. The proxy server then redirects the print job to the correct iPrint server.

For example, Juan is a laptop user and has installed and printed to a variety of iPrint printers at the company's headquarters.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

While on the road, Juan wants to submit a report to his boss. Rather than sending the report by e-mail or fax, Juan decides to send it to the printer near his boss.

When he tries to send the report to the printer, he receives an error that the printer cannot be found. He knows that the company uses a firewall and a proxy server.

He types the proxy server address in the iPrint Proxy settings, and then tries to print the report again. This time the print job is accepted.

The print job travels from his laptop to the proxy server. The proxy server redirects the print job to the printer's Print Manager, where the print job is spooled and forwarded to the printer.

To set the proxy server address in iPrint, do the following:

1. Select **Start > Programs > Novell iPrint > iPrint Settings > Proxy**.
2. Select the ***check box***; then enter the URL for the proxy server.
3. Select **OK**.

To disable using a proxy server, deselect the check box.

Manage Passwords for Remote iPrint Servers

You can manage passwords for print services that you indicate should be remembered by your workstation. The ability to delete passwords is useful if you are connected to a print service that you no longer use.

To manage passwords for print services, do the following:

1. Select **Start > Programs > Novell iPrint > iPrint Settings > Passwords**.
2. Select the ***password*** you want to remove; then select **Clear Password**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Manage iPrint's System Tray Icon

The iPrint icon in the system tray lets you receive notification when a job has printed and view a list of print jobs that you have submitted.

Do the following:

1. Select **Start > Programs > Novell iPrint > iPrint Settings > Tray Icon**.
2. Modify the following settings:
 - **iPrint Settings.** Opens the iPrint Client Settings.
 - **Document Status.** Lets you check the status and other information for the last 10 documents printed.
 - **Launch Printer Folder.** Opens the Windows printer folder.
 - **Find/Install Printers.** (Optional) Opens a browser window to the Menu Link URL specified on the Tray Icon tab.
 - **Close.** Removes the iPrint icon from the System Tray until the next reboot.

 To make the icon reappear in your system tray, select **Start > Programs > Novell iPrint > iPrint Client Settings > Tray Icon**; then deselect the **Enable the iPrint** icon in the system tray and select **OK**.

 Repeat Steps 1 and 2 to enable the icon.

Manage Print Job Notifications

iPrint can notify you when your document has printed or needs attention by way of a pop-up message in the system tray.

To turn iPrint notification on or off, do the following:

1. Select **Start > Programs > Novell iPrint > iPrint Settings > Notifications**.
2. Select or deselect the ***check box*** as indicated.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If you close the iPrint applet running in the system tray, you do not receive notifications. To restart the applet, see “Manage iPrint’s System Tray Icon” on 7-44.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 4 Migrate iPrint on NetWare to OES Linux

This objective explains how to copy existing iPrint Printer Agents or Print Managers (PSMs) running on NetWare 6.5 to iPrint Print Managers running on an OES Linux server.

To perform this task, you need to know the following:

- Migration Guidelines
- Migration Requirements
- How to Migrate iPrint Print Managers and Printer Agents Using the Server Consolidation Utility
- Post Migration Tasks

Migration Guidelines

When migrating an iPrint print system from NetWare to OES Linux, be aware of the following:

- The Server Consolidation Utility lets you copy existing iPrint printers running on NetWare to iPrint Managers running on OES Linux.

 NDPS printers can also be copied to a Print Manager on an OES Linux server, provided they are iPrint enabled first.

- Using the Server Consolidation Utility interface, you can merge the Printer Agents associated with an existing Print Manager on NetWare with the printers associated with an existing Print Manager on Linux.

 You can also create new Print Managers on Linux. With careful planning, you can easily migrate printers with no interruption to your users.

- The utility does not move nonreferenced objects such as driver profiles and custom banners.

- Print Managers and Printer Agents are not removed from the source server when you copy them. The print configuration is copied to the destination, not moved.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

When you are finished migrating your print system, you must manually delete the source Print Managers and Printer Agents (if you want them removed).

- When you move the Print Manager or Printer Agents to an OES Linux server, the printer objects are copied to the same eDirectory container as the Print Manager, even if the printer objects are distributed throughout the tree.

 This helps the Print Manager run more efficiently and avoids unnecessary calls to eDirectory for printer information.

- If you made changes to the iprint.ini file (located in sys:\apache2\htdocs\ippdocs\), you should copy the file to /var/opt/novell/iprint/htdocs/ on the destination server.

- iPrint maps and custom images are not migrated. If you are hosting these on your iPrint server, you need to copy them to the destination server.

Migration Requirements

During the migration, printer drivers are copied from the Resource Management Service (RMS) to the iPrint Driver Store (IDS).

For the migration to be successful, the following is required:

- The Resource Management Service (RMS) used by the Print Manager on a NetWare server must be up and running.
- The iPrint Driver Store (IDS) on an OES Linux server must be up and running.
- You must use an eDirectory user with sufficient rights to access the source and destination print system and eDirectory access permissions.
- DNS must be properly configured for the existing print system.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How to Migrate iPrint Print Managers and Printer Agents Using the Server Consolidation Utility

To migrate your iPrint print system, you need to complete the following tasks using the Server Consolidation Utility, which is launched from the Server Consolidation and Migration Toolkit:

1. If you have not already done so, install the iPrint Client on the workstation where you will be running the Server Consolidation Utility.

 The Server Consolidation Utility checks for the correct iPrint Client version and warns you if you need to install a newer version.

2. Make sure both Print Managers are running on the source and destination servers

 If you don't do this, you will get unpredictable results.

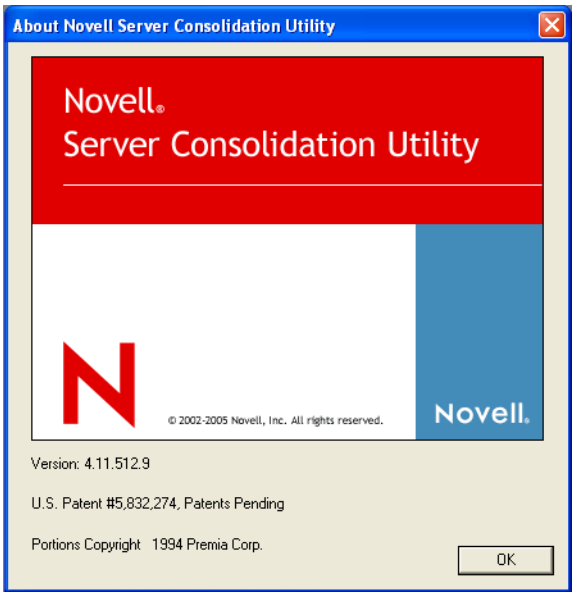
3. Start the Server Consolidation and Migration Toolkit and select the following options:

 - **NetWare or Open Enterprise Server (eDirectory)**
 - **Consolidate and Copy Data and Printing Between Servers**

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

When the Server Consolidation Utility launches, the following appears:

Figure 7-10

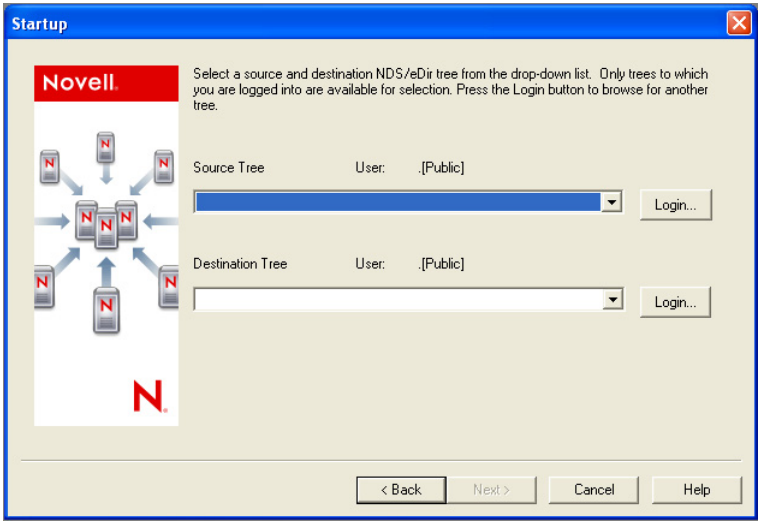


4. Select **OK**.
5. Select **Create a New Project**; then select **OK**.
6. Enter a ***project filename***; then select **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 7-11

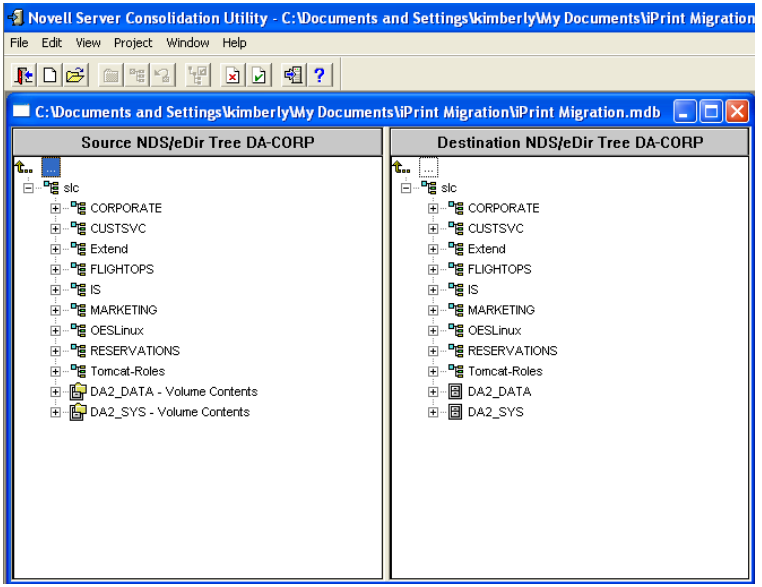


7. Select the desired ***NetWare source server*** and ***OES Linux destination server***; then select **Next**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The project window for your project appears (similar to the following:

Figure 7-12



8. From the project window, do one of the following to model your iPrint migration:

 - Drag-and-drop a Print Manager from the NetWare source tree onto a container in the Linux destination tree.



If the source and destination servers are in the same tree, you must copy the Print Manager to a different container than the one currently storing the Print Manager object.

By doing this, you are indicating that you want to create a new Print Manager in the specified container.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You are prompted to enter the following information about the new Print Manager:

Table 7-3

Parameter	Description
eDirectory Server	The server that all eDirectory (LDAP) calls are sent to. You can use the Browse button to locate this object in the tree.
Driver Store	The iPrint Driver Store on Linux that is to be associated with the new Print Manager. You can use the Browse button to locate this object in the tree.
DNS Name or IP Address	It is recommended that you associate the Print Manager with the DNS name of the OES Linux server that the Print Manager is loaded on. The other option is to specify the IP address of the OES Linux server. You must manually type the address; there is no browser for this information.

- Drag-and-drop individual Printer Agents from a Print Manager on NetWare onto a Print Manager on Linux.

 This indicates that you want to copy the Printer Agents from the source Print Manager to the specified destination Print Manager.



IMPORTANT: Dropping Printer Agents from a single Printer Manager to multiple Print Managers requires users to delete and reinstall the dropped iPrint printers.

or

- Drag-and-drop a Print Manager onto an existing Print Manager on Linux.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

This indicates that you want to copy all the Printer Agents for the source Print Manager to the specified destination Print Manager.

If you have already dropped individual Printer Agents for the Print Manager, you are warned that this is not allowed. You can back out the individually dropped printers and try the operation again.

9. Start the migration by selecting **Project > Verify and Copy Data**.

 The utility checks to make sure that it can communicate with the source Resource Management Service and the destination Driver Store, and that the moves you want to make are valid.

 To ensure a smooth migration, resolve all errors that are displayed before you proceed.

10. When you are ready to make the changes, run the consolidation by following the prompts.

 During the migration of secure printers, you might be prompted to enter the password for the secure printer if you have not selected the Remember Your Password option in the iPrint client.

11. When the migration is complete, review both the error and success log files.

 The log file uses the following states to identify the success of the migration of each Print Manager and Printer Agent:

 - **Success.** This indicates the Print Manager or Printer Agent was created on the destination server with all of its attributes and drivers.
 - **Partial Success.** This indicates the Print Manager or Printer Agent was created on the destination server but all some of its attributes and drivers were not included, so you should review its configuration.
 - **Failure.** This indicates the Print Manager or Printer Agent was not created on the destination server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Post Migration Tasks

When you are finished migrating your iPrint system, you might need to perform several tasks to complete the migration. This is especially true when migrating an iPrint system from a NetWare server to a Linux server.

These tasks include the following:

- **Edit the DNS records for the Print Manager.** You should have DNS records (an A record and a PTR record) configured on your DNS server for the Print Manager.

 These records are associated with an IP address that you need to change to reflect the IP address of the OES Linux server hosting the Print Manager.

- **Shut down the iPrint Broker and Print Manager on the NetWare server.** To make sure that all future iPrint activity is directed to the iPrint service on the OES Linux server, you should shut down the iPrint Broker and Print Manager on the NetWare server.

 You can do this by entering the following commands:

 unload ndpsm

 unload broker

- **Modify the autoexec.ncf file on the NetWare server.** Besides unloading the iPrint Broker and Print Manager, you will probably want to comment out or delete the command lines in the autoexec.ncf file to prevent these services from loading the next time you shut down or restart your NetWare server.

- **Delete the printer objects for the DA2 NetWare server.** Although this is not necessary, we recommend removing all objects from an eDirectory tree that are no longer useful to prevent any confusion when performing eDirectory configuration and maintenance tasks.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Edit the DA-PrintMgr.Linux.printers.da.ipsmd.conf file on the Linux server.** The DNS name that the iPrint server uses on an OES Linux server is stored in the ***printmgr_dn_name*.ipsmd.conf** file in the /etc/opt/novell/iprint/conf directory on the Linux server, where ***printmgr_dn_name*** is the DN (distinguished name) of the Print Manager eDirectory object.

 During migration, the PSMHostAddress parameter is normally changed. Open this file after migration to make sure the parameter is set to reflect the DNS name of the iPrint service.

 If you change the parameter, restart the iPrint service by entering rcnovell-ipsmd restart at a console prompt.

- **Update the certificate for the Print Manager on the Linux server.** After migration, you need to update the security certificate for the iPrint service on the Linux server.

 You can do this from iManager:

 1. Selecting **iPrint > Manage Print Manager**.
 2. Select the ***Print Manager object***.
 3. Selecting the **iPrint Certificate Manager** link.
 4. Select the **Allow the hostname *printmanager.example.com* to be used with this certification**, where ***printmanager.example.com*** is the DNS name of the Print Manager.

 When you finish this process, you need to start the Print Manager from iManager (**Manage Print Manager > *Print Manager name* > Startup**).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise 7-1 Migrate iPrint from the DA2 NetWare Server to the DA1 Linux Server

The Digital Airlines employees currently access office printers (such as an HP DeskJet printer) using iPrint running on the DA2 NetWare server.

You decide to migrate the iPrint service from the DA2 NetWare server to the DA1 Linux server.

To make this transition as smooth as possible, you want the employees to leave work on Friday and return to work on Monday still able to use any existing iPrint printers installed on their workstations without having to re-install the printers (a seamless migration).

You accomplish this by performing the following tasks:

- Configure the DA-PrintMgr Printer Manager for DNS
- Install the iPrint client and an iPrint printer on the Windows XP Professional workstation
- Prepare the DA1 Linux server for iPrint migration
- Migrate the iPrint service
- Complete post-migration tasks
- Verify that you can still use the HP-DJ printer on the Windows XP Professional workstation

In addition, you learn how to enable iPrint printing on Novell's latest workstation software, SUSE Linux Enterprise Desktop 10.

Exercise 7-1 Migrate iPrint from the DA2 NetWare Server to the DA1 Linux Server is in your *Integrating Novell Open Enterprise Server for Linux Workbook* on page 7-2.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Summary

Objective	Summary
1. Describe the Purpose and Architecture of iPrint	To describe the purpose and architecture of iPrint, you learned about the following: ■ **What iPrint Is.** iPrint lets mobile employees, business partners, and customers access printers from a variety of remote locations using existing Internet connections. Using a web browser, users point to a web page that displays the available printers for installation. ■ **iPrint components on Linux.** The following are the iPrint components on an OES Linux server: ■ Print Manager ■ Driver Store ■ iPrint Client ■ Apache Web Server ■ Novell iManager ■ **iPrint components on NetWare.** Novell iPrint on NetWare uses the NDPS (Novell Distributed Print Services) infrastructure. In addition to NDPS, iPrint uses the following components on NetWare: ■ Print Broker ■ Printer Drivers ■ Printer Objects ■ Print Manager

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
1. Describe the Purpose and Architecture of iPrint (*continued*)	■ iPrint Client ■ HTML pages ■ **iPrint port usage.** iPrint can use any port specified on Apache; however, iPrint defaults to two primary ports: ■ **Port 443.** All secure printing occurs over port 443 using SSL. ■ **Port 631.** All non-secure printing occurs over port 631.
2. Set Up and Manage the iPrint Server on OES Linux	To set up and manage iPrint on an OES Linux server, you learned how to do the following: ■ **Set up the iPrint Server on OES Linux.** If you select iPrint during a Novell OES Linux server installation (the default setting), the iPrint software components are automatically installed on your OES Linux server. To set up the iPrint server, you need to do the following: ■ Create a Driver Store ■ Add Printer drivers ■ Create a DNS name for the Print Manager ■ Create a Print Manager ■ Create a printer ■ **Manage the Print Manager.** The Print Manager uses a database to store information about the printers it controls.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
2. Set Up and Manage the iPrint Server on OES Linux (*continued*)	When you create a Print Manager, a configuration file is created in /etc/opt/novell/iprint. The file name is *print_manager_name*.ipsmd.conf. A separate file is created for each Print Manager that is created and assigned to run on the same server. Only one Print Manager can run on the server at a time. ■ **Manage Printers.** Although the default settings let users print without additional configuration, you might want to modify some of those settings so that you can manage your printing resources most effectively by doing the following: ■ Create additional printers ■ Manage printer agents ■ Use Printer Driver Profiles ■ Enable iPrint Direct ■ Manage print jobs ■ **Manage the Driver Store.** When you create a Driver Store, a configuration file is created in /etc/opt/novell/iprint. The file name is idsd.conf. Each time you create a Driver Store object using iManager and assign it to the same server, a separate entry is added to idsd.conf. Although you can have several Driver Stores assigned to a server, all printer driver files are stored in one file structure on the server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
3. Install and Configure the iPrint Client	To install and configure the iPrint client, you learned how to do the following: ■ **Install the iPrint client on Linux.** For iPrint to work properly, a workstation must have the iPrint client installed. You can distribute the client to workstations in a variety of ways, such as using the iPrint Printer List web page, using distribution software like ZENworks, or creating login scripts. To install the iPrint client on Linux, you need to know the following: ■ iPrint client requirements ■ Access control to the Workstation print system ■ How to install the iPrint client and your first printer on Linux ■ **Install the iPrint client on Windows.** To install the iPrint client on Windows, you need to know the following: ■ iPrint client requirements ■ iPrint client installation files ■ How to distribute the iPrint client for Windows ■ How to install a printer

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
3. Install and Configure the iPrint Client (*continued*)	■ **Configure the iPrint client settings.** To configure iPrint client settings, you need to know how to do the following: ■ Use a Proxy server ■ Manage passwords for remote iPrint servers ■ Manage iPrint's system tray icon ■ Manage print job notifications
4. Migrate iPrint on NetWare to OES Linux	In this objective you learned how to copy existing iPrint Printer Agents or Print Managers (PSMs) running on NetWare 6.5 to iPrint Print Managers running on an OES Linux server. To perform this task, you learned about the following: ■ **Migration guidelines.** When migrating an iPrint print system from NetWare to OES Linux, you need to be aware of issues that can impact the migration. ■ **Migration requirements.** For the migration to be successful, the following is required: ■ The Resource Management Service used by the Print Manager on a NetWare server must be up and running. ■ The iPrint Driver Store on an OES Linux server must be up and running.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
4. Migrate iPrint on NetWare to OES Linux (*continued*)	■ You must use an eDirectory user with sufficient rights to access the source and destination print system and eDirectory access permissions. ■ DNS must be properly configured for the existing print system. ■ **How to migrate iPrint Print Managers and Printer Agents using the Server Consolidation Utility.** To migrate your iPrint print system, you need to use the Server Consolidation Utility, which is launched from the Server Consolidation and Migration Toolkit. ■ **Post migration tasks.** When you are finished migrating your iPrint system, you might need to perform several tasks to complete the migration. This is especially true when migrating an iPrint system from a NetWare server to a Linux server. These include tasks such as editing the DNS records for the Print Manager and shutting down the iPrint Broker and Print Manager on the NetWare server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

SECTION 8 Install and Configure iFolder on an OES Linux Server

In this section, you learn how to install, configure, and use iFolder 3.*x* on an OES Linux Server.

Objectives

1. Describe the Purpose and Architecture of iFolder 3.x
2. Plan for an iFolder Services Installation
3. Install Novell iFolder 3.x and iFolder Web Access
4. Manage iFolder 3.x as an Administrator
5. Manage iFolder 3.x as a User

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Introduction

Novell iFolder 3.*x* is the next generation of iFolder, supporting multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution.

With iFolder, users' local files automatically follow them everywhere—online, offline, all the time—across computers. Users can share files in multiple iFolders, and they can share each iFolder with a different group of users.

Users control who can participate in an iFolder and their access rights to the files in it. Users can also participate in iFolders that others share with them.

In this section, you learn the fundamentals of how to install, configure, and use the iFolder 3.***x*** server, client, and iFolder Web access.



Although the current version of iFolder in Novell OES SP2 is iFolder 3.2, iFolder is referred to as iFolder 3.*x* throughout the course documentation and workbook because many of the features and administration tasks refer to all versions of iFolder 3, and product documentation refers to the service as iFolder 3.*x*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 1 Describe the Purpose and Architecture of iFolder 3.*x*

To describe the purpose and architecture of iFolder 3.*x*, you need to know the following:

- Benefits of iFolder for the Enterprise
- Benefits of iFolder for Users
- Enterprise Server Sharing
- How iFolder 3.x Works
- Key Components of iFolder

Benefits of iFolder for the Enterprise

Benefits of iFolder to the enterprise include the following:

- Seamless Data Access
- Data Safeguards and Data Recovery
- Reliable Data Security
- Productive Mobile Users
- Cross-Platform Client Support
- Scalable Deployment
- Simple Data and Account Management
- No Training Requirements

Seamless Data Access

Novell iFolder greatly simplifies your IT department's ability to keep users productive. It empowers users by enabling their data to follow them wherever they go.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The days of users emailing themselves project files so they can work on them from home are gone, as is the frustration associated with sorting through different versions of the same file on different machines.

iFolder stores and synchronizes users' work in such a way that no matter what client or what location they log in from, their files are available and in the condition that they expect them to be.

Users can access the most up-to-date version of their documents from any computer using the iFolder client or Web access.

Data Safeguards and Data Recovery

With Novell iFolder, data stored on the server can be easily safeguarded from system crashes and disasters that could result in data loss.

When a user saves a file locally, the iFolder client can automatically update the data on the iFolder server, where it immediately becomes available for an organization's regular network backup operations.

iFolder makes it easier for IT managers to ensure that all of an organization's critical data is protected.

Reliable Data Security

With Novell iFolder, LDAP-based authentication for access to stored data helps prevent unauthorized network access.

Productive Mobile Users

A Novell iFolder solution makes it significantly easier to support mobile users.

VPN connections are no longer needed to deliver secure data access to mobile users. Authentication and data transfer use Secure Sockets Layer (SSL) technology to protect data on the wire.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Users do not need to learn or perform any special procedures to access their files when working from home or on the road.

iFolder does away with version inconsistency, making it simple for users to access the most up-to-date version of their documents from any connected desktop, laptop, web browser, or handheld device.

In preparation to travel or work from home, users no longer need to copy essential data to their laptops from various desktop and network locations.

The iFolder client can automatically update a user's local computer with the most current file versions. Even when a personal computer is not available, users can access all their files via Web access with any computer connected to the Internet.

Cross-Platform Client Support

The iFolder client is available for Linux, Windows, and Macintosh desktops.

The Novell iFolder 3.*x* Web Access server provides a Web interface that allows users to access their files on the enterprise server with a Web browser from any computer with an active network or Internet connection.

Scalable Deployment

iFolder easily scales from small to large environments. You can install iFolder on multiple servers, allowing your iFolder environment to grow with your business.

A single iFolder enterprise server handles up to 1,000 user accounts, depending on the amount of memory and storage available.

Users in an LDAP context can be concurrently provisioned for iFolder services simply by assigning the context to an iFolder server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Simple Data and Account Management

Management of all iFolder enterprise servers is centralized through the Novell iFolder 3 plug-in to Novell iManager 2.5. Novell iFolder allows management from any location, using a standard Web browser.

iFolder also frees IT departments from routine maintenance tasks by providing secure, automatic synchronization of local files to the server.

No Training Requirements

IT personnel no longer need to condition or train users to perform special tasks to ensure the consistency of data stored locally and on the network.

With Novell iFolder, users simply store their files in the local iFolder directory. Their files are automatically updated to the iFolder server and any other workstations that share the iFolder.

iFolder works seamlessly behind the scenes to ensure that data is protected and synchronized.

Benefits of iFolder for Users

Typically, when users work in multiple locations or in collaboration with others, they must conscientiously manage file versions.

With iFolder, the most recent version of a user's files can follow the user to any computer where the iFolder client is installed and a shared iFolder is set up.

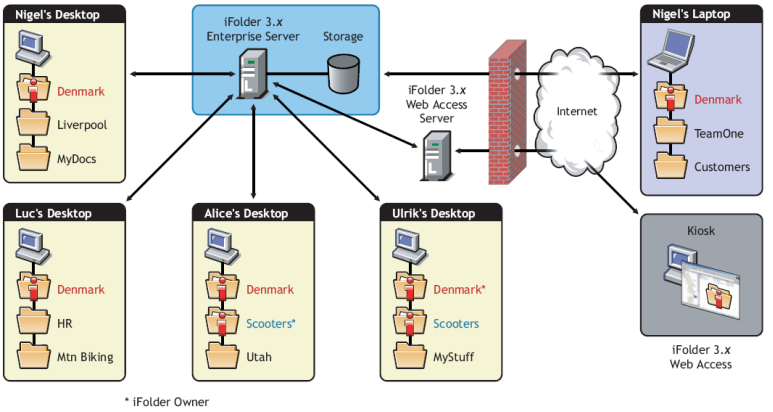
iFolder also allows users to share multiple iFolders and their separate content with other users of the iFolder system. Users decide who participates in each shared iFolder and what their level of access is.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Similarly, users can participate in shared iFolders that are owned by others in the collaboration environment.

In the following example, Ulrik owns an iFolder named Denmark and shares it via his iFolder enterprise account with Nigel, Luc, and Alice:

Figure 8-1



Nigel travels frequently, so he also set up the iFolder on his laptop. Any iFolder member can upload and download files from the Denmark iFolder from anywhere, using the iFolder Web Access server.

In addition, Alice shares a non-work iFolder named Scooters with her friend Ulrik.

With an enterprise server, the iFolders are stored centrally for all iFolder members. The iFolder server synchronizes the most recent version of documents to all authorized users of the shared iFolder.

All that the iFolder owner and iFolder members need is an active network connection and the iFolder client.

Novell iFolder provides the following benefits for users:

- Guards against local data loss by automatically backing up local files to the iFolder server and multiple workstations

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

- Transparently updates a user's iFolder files to the iFolder enterprise server and multiple member workstations with the iFolder client
- Tracks and logs changes made to iFolder files while users work offline, and synchronizes those changes when they go online
- Provides access to user files on the iFolder server from any workstation without the iFolder client, using a web browser and an active Internet or network connection
- With SSL encryption enabled, protects data as it travels across the wire
- Makes files on the iFolder server available for regularly scheduled data backup



For additional information on user benefits, see "Benefits of iFolder" on page 11 in the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Enterprise Server Sharing

The iFolder client included in this release supports synchronization across multiple computers through a central Novell iFolder 3.*x* enterprise server, which provides the following benefits and features:

- Users can share files across computers.
- Users can share files with others.
- Each user can own multiple iFolders.
- Each user can participate in multiple iFolders owned by other users.
- Files can be synchronized via the central server at any time and with improved availability, reliability, and performance.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

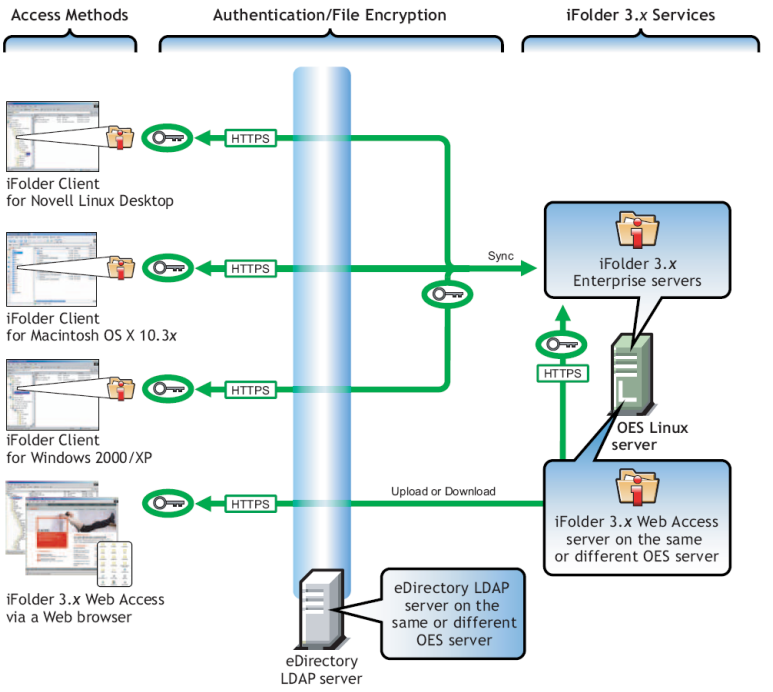
- Data is transferred securely over the wire using SSL connections.
- Users are autoprovisioned for iFolder services based on their assignment to administrator-specified LDAP containers and groups.
- A list of iFolder users is synchronized at regular intervals with the LDAP directory services.
- Local files are automatically backed up to the server at regular intervals and on demand.
- iFolder data on the server can be backed up to backup media and restored.
- Administrators can manage the iFolder system, user accounts, and user iFolders using the Novell iFolder 3 plug-in for iManager.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

How iFolder 3.x Works

Novell iFolder 3.*x* supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution, as illustrated in the following:

Figure 8-2



The following explains the information illustrated in Figure 8-2:

- **Access methods.** Linux, Macintosh, and Windows workstation users who have the Novell iFolder client installed can access and modify their files in one or more workstation folders.

 Changes are automatically synchronized with the iFolder 3.*x* Enterprise servers.

 A web interface lets users access their files from any computer with an active network or Internet connection.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Authentication/file encryption.** All file service access is controlled by LDAP-based authentication through the eDirectory LDAP server.

 Although shown separately, eDirectory could be installed on the OES server.

 Files can be encrypted for transport using SSL connections (HTTPS).

- **Novell iFolder services.** Local and network copies of each file are automatically synchronized by the Novell iFolder client and server components.

Key Components of iFolder

The following are the key components of iFolder 3.*x*:

- iFolder Enterprise Server
- Novell iFolder 3 Plug-In for Novell iManager 2.5
- iFolder Web Access
- The iFolder Client
- Shared iFolders
- iFolder Access Rights
- Account Setup for Enterprise Servers
- Access Authentication
- File Synchronization and Data Management
- Synchronization Log
- iFolder Client APIs

iFolder Enterprise Server

The iFolder enterprise server is a central repository for storing iFolders and synchronizing files for enterprise users.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell iFolder 3 Plug-In for Novell iManager 2.5

The Novell iFolder 3 plug-in for Novell iManager 2.5 is an administrative tool you use to manage the iFolder system, user accounts, and user iFolders and data.

iFolder Web Access

The iFolder 3.*x* Web Access server provides an interface to allow users remote access to iFolders on the enterprise server.

The iFolder Client

The iFolder client integrates with the user's operating system to provide iFolder services in a native desktop environment. It supports the following client operating systems:

- Novell Linux Desktop 9
- SUSE Linux Enterprise Desktop 10 (SLED 10)
- Windows 2000/XP
- Macintosh OS X v10.3 or later

An iFolder session begins when the user logs in to an iFolder services account and ends when the user logs out of the account or exits the iFolder client.

The iFolders synchronize files with the enterprise server only when a session is active and the computer has an active connection to the network or Internet.

Users can access data in their local iFolders at any time; it does not matter if they are logged in to their server accounts or if they are connected to the network or Internet.

The iFolder client allows users to create and manage their iFolders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Shared iFolders

An iFolder is a local directory that the user selectively shares with other users in a collaboration environment.

The iFolder files are accessible to all members of the iFolder and can be changed by those with the rights to do so. Users can share iFolders across multiple workstations and with others.

Because the iFolder client is integrated into the operating environment, users can work with iFolders directly in a file manager or in the My iFolders window.

Within the iFolder, users can set up any subdirectory structure that suits their personal or corporate work habits. The subdirectory structure is constant across all member iFolders.

Each workstation can specify a different parent directory for the shared iFolder.

iFolder Access Rights

The iFolder client provides four levels of access for members of an iFolder:

- **Owner.** Only one user serves as the owner. This is typically the user who created the iFolder.

 The owner or an iFolder administrator can transfer ownership status from the owner to another user.

 The owner of an iFolder has the Full Control right. This user has read/write access to the iFolder, manages membership and access rights for member users, and can remove the Full Control right for any member.

 With an enterprise server, the disk space used by the owner's iFolders count against the owner's user disk quotas on the enterprise server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If a user is deleted as a user for the iFolder system, the iFolders owned by the user are orphaned. Orphaned iFolders are assigned temporarily to the iFolder Admin user, who becomes the owner of the iFolder.

Membership and synchronization continues while the iFolder admin user determines whether an orphaned iFolder should be deleted or assigned to a new owner.

- **Full Control.** A member of the shared iFolder, with the Full Control access right. The user with the Full Control right has read/write access to the iFolder and manages membership and access rights for all users except the owner.
- **Read/Write.** A member of the shared iFolder, with the Read/Write access right to directories and files in the iFolder.
- **Read Only.** A member of the shared iFolder, with the Read Only access right to directories and files in the iFolder. This member can copy an iFolder file to another location and modify it outside the iFolder.

When used with an enterprise server account, the server hosts every iFolder created for that account.

Users can create an iFolder and the enterprise server makes it available to the specified list of users. A user can have a separate account on each enterprise server. A user's level of membership in each shared iFolder can differ.

Account Setup for Enterprise Servers

The iFolder client lets you set up multiple accounts, with one each allowed per enterprise server. Users specify the server address, username, and password to uniquely identify an account.

On his or her computer, a user sets up accounts while logged in as the local identity he or she plans to use to access that account and its iFolders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Under the local login, the user can set up multiple iFolder accounts, but each account must belong to a different iFolder enterprise server.

Access Authentication

Whenever iFolder connects to an enterprise server to synchronize files, it connects to the server using HTTP BASIC and SSL, and the server authenticates the user against the LDAP directory service.

File Synchronization and Data Management

When you set up an iFolder account, you can enable Remember Password so that iFolder can synchronize iFolder invitations and files in the background as you work.

The iFolder client runs automatically each time you log in to your computer's desktop environment. The session runs in the background as you work with files in your local iFolders, tracking and logging any changes you make.

With an enterprise server, you can synchronize the files at specified intervals or on demand.

Synchronization Log

The log displays a log file of your iFolder background activity.

iFolder Client APIs

As part of the iFolder project, APIs are available for the client.

For iFolder Client developer documentation, see the iFolder Software Developers Kit at http://forge.novell.com/modules/xfmod/docman/?group_id=1372.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 2 Plan for an iFolder Services Installation

In this objective, you are introduced to planning considerations for providing Novell iFolder 3.*x* services on OES Linux. These include the following:

- Security Considerations
- Server Workload Considerations
- Naming Conventions for Usernames and Passwords
- Admin User Considerations
- iFolder User Account Considerations
- iFolders Data and Synchronization Considerations
- Management Tools

Security Considerations

For information about planning security for your iFolder 3.*x* system, see the *Novell iFolder 3.x Security Administrator Guide*.



You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Server Workload Considerations

The iFolder 3.*x* enterprise server supports a complex usage model in which each user can own multiple iFolders and participate in iFolders owned by other users.

Instead of a single user working from different workstations at different times, multiple users can be concurrently modifying files and synchronizing them.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Whenever a user adds a new member to an iFolder, the workload on the server can increase almost as much as if you added another user to the system.

We recommend a maximum of 1,000 users per iFolder server, depending on the performance characteristics of your hardware.

You can set user account quotas to control the maximum storage space consumed by a user's iFolders on the server.

The actual bandwidth usage for each iFolder depends on the following:

- The number of members subscribed to the iFolder
- The number of computers actively sharing the iFolder
- How much data is stored in the iFolder
- The actual and average size of files in the iFolder
- The number of files in the iFolder
- How frequently files change in the file
- How much data actually changes
- How frequently files are synchronized
- The available bandwidth and throughput of network connections

We recommend that you set up a pilot program to assess your operational needs and performance based on your equipment and collaboration environment, and then design your system accordingly.

The following is a suggested baseline configuration for an iFolder 3.*x* server with a workload similar to a typical iFolder 2.1 server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

It is based on an example workload of about 12.5 GB of data throughput (up and down) each 24 hours, including all Ethernet traffic and protocol overhead (your actual performance might differ):

Table 8-1

Component	Example System Configuration
Hardware	■ 1.8 GHz Single processor ■ 1.2 GB RAM ■ 300 GB hard drive
iFolder Services	■ 500 users ■ 500 MB user account quota per user ■ 1 iFolder per user that is not shared with other users ■ 5% change in each user's data per 24-hour period

Naming Conventions for Usernames and Passwords

The following are naming convention guidelines for usernames and passwords:

- LDAP Naming Requirement
- Email Address Naming Requirement
- Length and Format Considerations for an LDAP Object
- Multilingual Considerations

LDAP Naming Requirement

Usernames and passwords must comply with the constraints set by your LDAP service.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



For complete details, see the ***Novell eDirectory 8.7.3 Administration Guide*** (edir873.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Email Address Naming Requirement

If you configure iFolder to authenticate users at login based on their email addresses, make sure that each email address in eDirectory satisfies the following naming requirements:

- Conforms to standard email naming conventions
- Is unique in the directory

For example, if two identical email addresses exist in the directory, iFolder could synchronize both of them, but it attempts to authenticate only to the first matching email address it finds.

Authentication fails if the password does not match that address.

iFolder does not transform the address the user enters in any way and treats the names as case-sensitive. Your users should be aware of the format and case used for their email addresses that are stored in eDirectory.

For example, if user John Smith has an email address based on a user ID of js1234 (such as js1234@example.com), but is allowed to use an email alias such as john.smith@example.com, you need to decide which address the user should enter as the iFolder user name.

Length and Format Considerations for an LDAP Object

In iManager, the maximum number of characters for most LDAP objects is 64 characters. Some fields require common name format and others require fully distinguished name format for objects.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Review the iManager Help for the different plug-ins to make sure your entries comply with length and format restrictions for the individual plug-in.

Multilingual Considerations

If you have workstations running in different languages, you might want to limit user object names to characters that are viewable on all the workstations.

For example, a name entered in Japanese cannot contain characters that are not viewable in Western languages.



eDirectory supports only English language characters for usernames and passwords on Linux and HP-UNIX. This applies to OES Linux and Novell Linux Desktop.

For complete details, see “Multilingual Considerations” on page 70 in the *Novell eDirectory 8.7.3 Administration Guide* (edir873.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Admin User Considerations

During iFolder installation, iFolder creates two administrator users—the iFolder Admin user and the iFolder Proxy user.

After installation, you can also configure other users with the iFolder Admin right to make them equivalent to the iFolder Admin user.

To make decisions about how to set up admin users, you need to know the following:

- iFolder Admin User and Equivalent Users
- iFolder Proxy User

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

iFolder Admin User and Equivalent Users

The iFolder Admin user is the primary administrator of the iFolder enterprise server. Whenever iFolders are orphaned, ownership is transferred to the iFolder Admin user for reassignment to another user or for deletion.

You initially specify the iFolder Admin user during the iFolder enterprise server configuration in YaST.

The iFolder Admin user object must be created to enable the iFolder Admin to perform management tasks. iFolder tracks this user by the LDAP object GUID, allowing it to belong to any LDAP container or group in the tree, even those that are not identified as Search DNs.

The user's movement can be tracked anywhere in the tree because it is known by the GUID, not the user DN.

The iFolder Admin right can be assigned to other users so that they can also manage iFolder services for the selected server. Use the Administrators page in the Novell iFolder 3 plug-in to add or remove the iFolder Admin right for users.

Only users who are in one of the DNs specified in the LDAP Search DN are eligible to be equivalent to the iFolder Admin user.

If you assign the iFolder Admin right to other users, those users are governed by the roster and Search DN relationship.

The user is removed from the roster and stripped of the iFolder Admin right if you delete the user, remove the user's DN from the list of Search DNs, or move the user to a DN that is not in the Search DNs.

iFolder Proxy User

The iFolder Proxy user is the identity used to access the LDAP server to retrieve lists of users in the specified containers, or groups, or users that are defined in the iFolder LDAP settings.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

This identity must have the Read right to the LDAP directory. The iFolder Proxy user is created during the iFolder installation. You probably never need to modify this value.



If you do modify the iFolder Proxy user, make sure that the identity you specify is different than the iFolder Admin user or other system users because the iFolder Proxy user password is stored in reversible encrypted form in the Simias database on the iFolder server.

When you initially configure the iFolder enterprise server in YaST, iFolder autogenerates a password for the iFolder proxy user.

The following is the encryption method for the iFolder proxy user password:

Table 8-2

iFolder Version	Encryption Method	Proxy User Password
iFolder 3.2	YaST encryption method	Generates an alphanumeric, 13-digit, mixed-case password.
iFolder 3.0 and 3.1	BASH random number generator	Generates a number between 0 and 10,000 and appends it to iFolderProxy. For example, iFolderProxy1234.

Initially, the password for the iFolder Proxy user is stored in clear text in the /opt/novell/ifolder3/etc/simias-server-bootstrap.config file.

At the end of the configuration process, the system reboots Apache 2 and starts iFolder. When iFolder runs this first time after configuration, the iFolder process copies the simias-server-bootstrap.config file to the Simias.config file.

The default location of the Simias.config file is either the /var/lib/wwwrun/.local/share/simias directory or the /home/wwwrun/.local/share/simias directory.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The proxy user password is stored in a reversible encrypted form in the Simias database, and then the value is removed from both configuration files.

The password stored on the system for the iFolder Proxy user must match the password stored in the iFolder Proxy user's eDirectory object.

If you ever modify the iFolder Proxy user password in eDirectory, you must also change the password stored on the system.

For example, if you change the iFolder Proxy user assignment, or if you want to set a longer password for the iFolder Proxy user, you must modify the values afterwards in iFolder's LDAP settings or iFolder cannot access the LDAP server to update the user list.

To secure access to the Simias.config file, administrators of the iFolder 3.*x* server computer must use every precaution to not inadvertently assign unauthorized users file system rights to the /var/lib/wwwrun/.local/share/simias directory or the /home/wwwrun/.local/share/simias directory.

iFolder User Account Considerations

The following are guidelines you should consider when planning for iFolder user accounts:

- Preventing the Propagation of Viruses
- Provisioning User Accounts
- Setting Account Quotas

Preventing the Propagation of Viruses

Because iFolder is a cross-platform, distributed solution, virus infection could occur on Windows machines migrating across the iFolder server to other platforms, and vice versa.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You should enforce server-based virus scanning to prevent viruses from entering the corporate network.

You should also enforce client-based virus scanning.



For details, see "Configuring Local Virus Scanner Settings for iFolder Traffic" on page 46 in the *iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Provisioning User Accounts

You can specify any existing containers and groups in the Search DNs field of the iFolder LDAP settings to govern which users are automatically provisioned with accounts for iFolder services.

The LDAP synchronization tracks a user object's eDirectory GUID to identify the user in multiple contexts as you add, move, or relocate user objects, or as you add and remove contexts as Search DNs.

The following guidelines apply:

- If the user is added to an LDAP container, group, or user that is in the Search DN, the user is added automatically to the iFolder user list.
- If a user is moved to a different container and the new container is also in the Search DN, the user remains in the iFolder user list.

 If you intend to keep the user as an iFolder user without interruption of service and loss of memberships and data, the new container must be added as a Search DN before the user is moved.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If the user is moved to a different container that is not specified as a Search DN before the user is moved, the user is removed from the iFolder user list. The user's iFolders are orphaned and the user is removed as a member of iFolders owned by others.

If the new container is later added as a Search DN, the user is treated as a new user, with no association with previous iFolders and memberships.

- If the user appears in multiple defined Search DNs, and one or more DNs are removed from the LDAP settings, the user remains in the iFolder user list if at least one DN containing the user remains.
- If the user is deleted from LDAP or moved from all defined Search DNs, the user is removed as an iFolder user. The user's iFolders are orphaned and the user is removed as a member of iFolders owned by others.
- The iFolder Admin user and iFolder Proxy user are tracked by their GUIDs, whether their user objects are in a context in the Search DN or not.

Setting Account Quotas

You can restrict the amount of space each user account is allowed to store on the server by setting an account quota.

The account quota applies to the total space consumed by the iFolders the user owns. If the user participates in other iFolders, the space consumed on the server is billed to the owner of that iFolder.

You can set quotas at the system or user level. Within a given account quota, you can also set a quota for any iFolder.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

iFolders Data and Synchronization Considerations

Consider the following when setting policies for iFolders data and synchronization:

- Naming Conventions for an iFolder and Its Folders and Files
- Guidelines for File Types and Sizes to Be Synchronized

Naming Conventions for an iFolder and Its Folders and Files

The iFolder client imposes naming conventions that consider the collective restrictions of the Linux, Windows, and Macintosh file systems.

An iFolder, folder, or file must have a valid name that complies with the naming conventions before it can be synchronized.

Use the following naming conventions for your iFolders and the folders and files in them:

- iFolder supports the Unicode* (http://www.unicode.org) character set with UTF-8 encoding.
- Do not use the following invalid characters in the names of iFolders or in the names of folders and files in them:

 \/:*?"<>|;

 iFolder creates a name conflict if you use invalid characters in a file or folder name. The conflict must be resolved before the file or folder can be synchronized.
- The maximum name length for a single path component is 255 bytes. For filenames, the maximum length includes the dot (.) and file extension.
- Names of iFolders, folders, and files are case insensitive; however, case is preserved.

 If filenames differ only by case, iFolder creates a name conflict. The conflict must be resolved before the file or folder can be synchronized.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- If users create iFolders on the FAT32 file system on Linux, they should avoid naming files in all uppercase characters.

 The VFAT or FAT32 file handling on Linux automatically changes filenames from all uppercase characters to all lowercase characters that

 - Are all uppercase characters

 and

 - Meet the MS-DOS 8.3 file format

 This creates synchronization problems for those files if the iFolder is set with the Read Only access right.

Guidelines for File Types and Sizes to Be Synchronized

You can set policies to govern which files are synchronized by specifying file type restrictions and the maximum file size allowed to be synchronized.

You can set these policies at the system, user account, and iFolder level.

Some file types are not good candidates for synchronization, such as operating system files, hidden files created by a file manager, or databases that are implemented as a collection of linked files.

You might include only key file types used for your business or exclude files that are likely unrelated to business, such as .mp3 files.

Consider the following:

- Operating System Files
- Hidden Files
- Database Files
- File Sizes

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Operating System Files

You should not convert system directories to iFolders. Most system files change infrequently and it is better to keep an image file of your basic system and key software than to attempt to synchronize those files to the server.

Hidden Files

If your file system uses hidden files to track display preferences, you should determine the file types of these files and exclude them from being synchronized on your system.

Usually, they are relevant only to the particular computer where they were created, and they change every time the file or directory is accessed.

You do not need to keep these files, and synchronizing them results in repeated file conflict errors.

For example, iFolder automatically excludes two hidden file manager files called thumbs.db and .DS_Store.

Database Files

iFolder synchronizes the changed portions of a file; it does not synchronize files as a set.

If you have a database file that is implemented as a collection of linked files, do not try to synchronize them in an iFolder.

Do not try to synchronize your GroupWise data by making the GroupWise archive, cache, or remote directories into iFolders.

If you do this, the GroupWise data files become corrupted after being synchronized a few times. GroupWise needs the files in the archive to be maintained as a set of files.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

File Sizes

The maximum file size you allow for synchronization depends on your production environment.

While some users work with hundreds of small files, other users work with very large files. You might set a system-wide policy to restrict sizes for most users, and then set individual policies for power users.

Management Tools

You use the following tools to manage the Novell iFolder 3.*x* enterprise server and Web Access server:

- iFolder Configuration Plug-Ins for YaST
- Novell iFolder 3 Plug-In for Novell iManager 2.5
- Web Access Configuration File

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

iFolder Configuration Plug-Ins for YaST

iFolder provides the following plug-ins to YaST for configuring basic parameters for your iFolder system:

Table 8-3

iFolder Plug-in	Purpose	Task
iFolder 3	Use this function to configure the following parameters for the iFolder enterprise server: ■ LDAP server name, LDAP admin DN, and password ■ iFolder system name, store path, and description ■ iFolder proxy DN, password, and search context for retrieving user information from LDAP ■ iFolder admin DN and password	In YaST, select **Network Services**; then select **iFolder 3**.
iFolder Web Access	Use this function to configure the following parameters for the iFolder Web Access server: ■ Web Access alias ■ iFolder server URL	In YaST, select **Network Services**; then select **iFolder 3 Web Access**.

If both iFolder components are installed on the same computer, both plug-ins are available; otherwise, only the plug-in that is needed is available.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell iFolder 3 Plug-In for Novell iManager 2.5

The Novell iFolder 3 plug-in for Novell iManager 2.5 is an administrative tool used to manage the iFolder system, user iFolder accounts, and user iFolders and data.

Before you can use Novell iFolder 3 for managing your iFolder system, you must install it in iManager.

An iManager plug-in might not operate properly if the highest priority Language setting for your web browser is set to a language other than one of the supported languages.

To avoid problems, in your web browser's Languages setting, set the first language preference in the list to a supported language, such as English.



In the initial release, iFolder supports only English. Localization in additional languages is planned for future releases.

Web Access Configuration File

Use the /opt/novell/ifolder3/webaccess/Web.config file to configure HTTP runtime parameters for your iFolder Web Access server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 3 Install Novell iFolder 3.*x* and iFolder Web Access

To install Novell iFolder 3.*x* and iFolder Web Access, you need to know the following:

- Prerequisites and Installation Guidelines
- How to Install iFolder on an Existing OES Linux Server
- How to Configure the iFolder Enterprise Server
- How to Configure the iFolder Web Access Server
- How to Install the Novell iFolder 3 Plug-In for iManager
- How to Access iManager and the Novell iFolder 3 Plug-In
- How to Provision Users and iFolder Services

Prerequisites and Installation Guidelines

The following are prerequisites and guidelines for this release of Novell iFolder 3.*x* and the iFolder client included in Novell OES SP2.

Before installing and configuring iFolder, make sure that your system meets the requirements in each of the following categories:

- File System
- Enterprise Server
- Novell eDirectory 8.7.3
- Novell iManager 2.5
- Mono
- Client Computers
- Web Browser

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

File System

iFolder 3.*x* installs the iFolder files on the system volume. OES Linux requires the Reiser (default) or EXT3 file system for the system device.

We recommend that you store the users' iFolder data on a separate volume.

The following are supported file systems based on iFolder version:

Table 8-4

Version	Data File System Support
iFolder 3.1 and later	EXT3, ReiserFS, or NSS
iFolder 3.0	EXT3 or ReiserFS

Enterprise Server

We recommend that you install iFolder 3.*x* Enterprise Server and Web Access server after your OES Linux system is configured and running properly.

You must post-install iFolder if you plan to use NSS volumes for your iFolder data because you cannot set up NSS volumes during an OES Linux installation.

However, if you plan to use a Linux traditional volume such as EXT3 or ReiserFS for your iFolder data, you can optionally install and configure iFolder when you install OES Linux.

The following are additional prerequisites and guidelines for iFolder Enterprise Server:

- Prerequisites for the Operating System
- Install Guidelines When Using an NSS Volume to Store iFolder Data
- Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Install Guidelines for Other Components

Prerequisites for the Operating System

Novell iFolder 3.2 and earlier is designed to work only on the Novell Open Enterprise Server for Linux (OES Linux) platform, which is comprised of specific versions of the SUSE Linux Enterprise Server platform and the basic OES applications and services.



iFolder 3.2 server and earlier does not support SUSE Linux Enterprise Server without the basic OES applications and services. It also does not support OES NetWare.

iFolder 3.*x* requires the following versions of the OES Linux server:

Table 8-5

iFolder Version	OES Linux Version
iFolder 3.2	Novell Open Enterprise Server Support Pack 2 for SUSE Linux Enterprise Server 9 Support Pack 3 (OES SP2 Linux)
iFolder 3.1	Novell Open Enterprise Server Support Pack 1 for SUSE Linux Enterprise Server 9 Support Pack 2 (OES SP1 Linux)
iFolder 3.0	Novell Open Enterprise Server for SUSE Linux Enterprise Server 9 Support Pack 1 (OES Linux)

There is no upgrade or migration path from Novell iFolder 2.1*x* and earlier versions of iFolder.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Install Guidelines When Using an NSS Volume to Store iFolder Data

Make sure you modify the OES Linux install and configuration to comply with the following guidelines:

- In YaST, on the Installation Settings page, reconfigure the Partitioning settings as needed to support using NSS:
 - Specify a ReiserFS (default) or EXT3 partition as your system device.
 - NSS volumes are configured after installation is complete.

 If you plan to use NSS volumes, some deployment scenarios require that you modify the partitioning to use EVMS (Enterprise Volume Management System) as the device manager of the system device instead of LVM (Linux Volume Manager, default) or a third-party volume manager.

 Make sure to compare your storage deployment plan to those listed in "Installing Linux with EVMS as the Volume Manager of the System Device" in the *OES Linux Installation Guide* to determine if you need to do this.

 For example, if you have only a single device on the server (such as a single physical disk or a hardware RAID 1 or RAID 5 device) and you plan to configure an NSS volume to use as your iFolder data volume, you must modify your partitioning to use EVMS to manage the device.
- In YaST, on the Installation Settings page, modify the Software components to add the NSS package to the installation.

 Plan to install iFolder after your OES Linux server is set up and you have created an NSS volume to use.
- In YaST, on the Installation Settings page, make sure you do not add the iFolder 3 or iFolder 3 Web Access components to the installation. You will install them later.
- After the OES Linux system is up and running, use the Storage plug-in to iManager to create the NSS volume, create a directory at the volume root, and then use YaST to install and configure iFolder.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Make sure to specify the path to the directory as the iFolder data store during the iFolder configuration.

Install Guidelines When Using a Linux Traditional Volume to Store iFolder Data

The following are installation guidelines when using a Linux traditional volume for iFolder data:

- In YaST, specify an EXT3 or ReiserFS partition as your system device.
- (Optional) Modify the Software components to add the iFolder 3 or iFolder 3 Web Access components to the installation.

If you install iFolder during OES Linux installation, be prepared to configure iFolder as part of the installation process.

Install Guidelines for Other Components

We recommend that your iFolder enterprise server and Web Access server run on separate dedicated servers. For small office use, both the enterprise server and the web access server can run on the same server without degraded performance.

For best performance, configure your iFolder server as an independent system with, at most, the following services:

- OES Linux (minimum predefined server plus graphics support and NSS if desired)
- Novell eDirectory 8.7.3 (can be configured on a different OES server)
- Novell iManager 2.5 (can be configured on a different OES server)
- Novell iFolder 3.*x* (typically post-installed on an OES Linux server)
- iFolder Enterprise server
- Web Access server (can be installed and configured on a different OES Linux server)

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Mono (The Mono package is required for iFolder 3.*x* enterprise server and for Web Access server.)
- Apache 2 Web Server (The apache2-worker package is required for iFolder 3.*x* enterprise server and for web access server.)
- Other iFolder dependencies as noted in YaST by the iFolder 3.*x* and iFolder 3.*x* Web Access install packages.

Installing other applications or services on the iFolder server affects iFolder performance and might introduce conflicts with the required versions of applications iFolder depends on, such as Apache 2 or Mono.

Novell eDirectory 8.7.3

Novell eDirectory 8.7.3 is a secure identity management solution that provides centralized identity management, infrastructure, Net-wide security, and scalability to all types of applications running behind and beyond the firewall.

It natively supports the directory-standard Lightweight Directory Access Protocol (LDAP) 3 and provides support for TLS/SSL services based on the OpenSSL source code.

eDirectory is available as a component of Novell OES.

Before you configure iFolder, eDirectory must be configured and running. In iFolder, you specify LDAP containers and groups that contain user objects of users that you want to be iFolder users. You must create contexts and define users in eDirectory.

Make sure your LDAP objects comply with the naming conventions for your LDAP services.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Novell iManager 2.5

Novell iManager 2.5 is a Web-based administration console that provides secure, customized access to network administration utilities and content.

Before you can configure the Novell iFolder 3 plug-in for iManager, iManager must be installed and configured.

Mono

Novell iFolder 3.*x* requires the Mono framework for Linux.

Mono is a development platform for running and developing modern applications. Based on the ECMA/ISO Standards, Mono can run existing programs that target the .NET or Java frameworks.

The Mono Project is an open source effort led by Novell and is the foundation for many new applications.



For details about Mono, see the Mono Project Web site at http://www.mono-project.com/Main_Page.

The required version of Mono is included on the .iso files. Mono is installed automatically as a dependency of iFolder during installation of the iFolder enterprise server or the Web Access server.

The iFolder clients for Linux and Macintosh also require Mono 1.1.7. The required version of Mono is packaged in the iFolder client installation files that you distribute to your users.

Linux and Macintosh users must install both iFolder and Mono packages.

Be sure to use the required version of Mono. If you have a different version of Mono on your OES Linux server, uninstall it before you install iFolder.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell iFolder 3.*x* supports only the version of Mono included in its install software. If you need to upgrade Mono for another reason, please check our online documentation to see if we explicitly support that version and to learn any necessary steps to make the upgrade work correctly.

Client Computers

The iFolder client supports the following workstation operating systems:

- Novell Linux Desktop 9 and later (requires Mono 1.1.7.1.44342 for Linux)
- SUSE Linux Enterprise Desktop 10 (requires Mono 1.1.7.1.44342 for Linux)
- Windows 2000/XP/2003 with the latest .NET support patches
- Macintosh OS X v10.3 and later (requires Mono 1.1.7.2 for Macintosh)

Make sure you have installed the latest critical updates for your operating system or .NET.

Web Browser

You need one of the following supported Web browsers on the computer you use to access iManager and on the client computers:

- Mozilla Firefox
- Microsoft Internet Explorer
- Safari on Macintosh

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How to Install iFolder on an Existing OES Linux Server

We recommend that you install iFolder after your server operating system is installed and all storage services are configured.

The following procedures describe how to install iFolder enterprise server, iFolder Web access server, or both on an existing OES Linux platform.

If you install only one of the iFolder servers, repeat the entire installation process for the other on a second OES Linux server.

To install the iFolder components using the YaST Install and Remove Software module, do the following:

1. Before you begin, make sure your OES Linux system setup meets the “Prerequisites and Installation Guidelines” on 8-32.
2. If you have previously installed Mono on your OES SP1 server, make sure the permissions on Mono directories are set correctly.

 The following steps should set the rights correctly for Mono, and enable iFolder 3.*x* enterprise server to run:

 a. From a terminal window on your Linux computer desktop, switch to the root user (enter **su -** and the ***root password***).

 b. At the command prompt, enter **cd /usr/lib**.

 c. Change the Mono permissions in the /usr/lib directory by entering **chmod 755 -R mono**.

 d. At the command prompt, enter **cd /etc**.

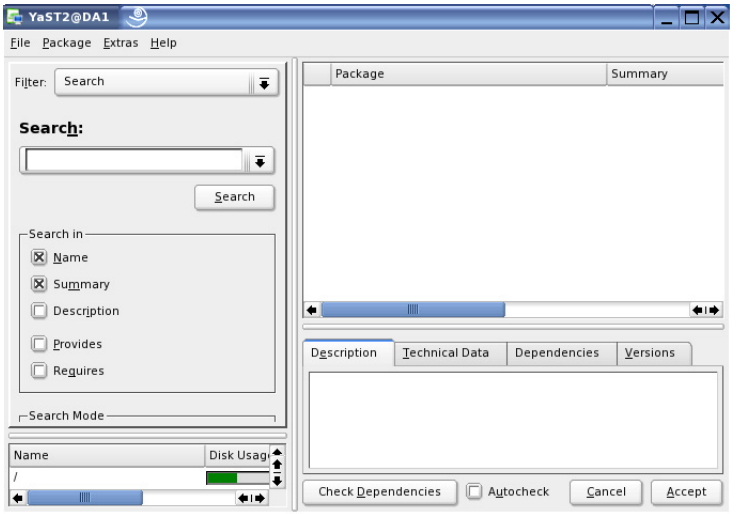
 e. Change the Mono permissions in the /etc directory by entering **chmod 755 -R mono**.
3. Open YaST by selecting the **YaST** icon (on your desktop); then enter the ***root password***.

 The Yast Control Center appears.
4. From the left, select **Software**; from the right, select **Install and Remove Software**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A window appears in the upper left with a Filter drop-down menu preselected to the Search option:

Figure 8-3



5. From the Filter drop-down menu, select the **Selections** option.

 A list of selections is displayed that includes the following (at the bottom):

 - Novell iFolder 3.*x* Web Access
 - Novell iFolder 3.*x*

 You can install the iFolder 3 Enterprise Server and Web Access Server on the same computer or on different computers.

6. Do one or both of the following, depending on your deployment preferences:

 - Select (check) **Novell iFolder 3.x** to indicate that you want to install the RPMs for Novell iFolder 3 and its dependencies.
 - Select (check) **iFolder 3.x Web Access** to indicate that you want to install the RPMs for Novell iFolder 3 Web Access and its dependencies.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If you install only one of the components, repeat the entire installation process for the other on your second server.

7. To begin the installation, select **Accept** (bottom right of the dialog).
8. (Conditional) If a dialog appears indicating any dependency conflicts, resolve them before continuing.
9. When the installation is complete, close the YaST Control Center.



If you have problems with Mono after the installation, check the POSIX permissions on Mono directories to make sure they comply with the settings in Step 2 of the installation.

Another method for installing iFolder 3.*x* and iFolder 3.*x* Web Access is to use the iFolder configuration icons in the YaST Control Center.

Do the following:

1. Before you begin, make sure your OES Linux system setup meets the “Prerequisites and Installation Guidelines” on 8-32.
2. If you have previously installed Mono on your OES SP1 server, make sure the permissions on Mono directories are set correctly.

 The following steps should set the rights correctly for Mono and enable iFolder 3.*x* enterprise server to run:

 a. From a terminal window on your Linux computer desktop, switch to the root user (enter **su -** and the ***root password***).
 b. At the command prompt, enter **cd /usr/lib**.
 c. Change the Mono permissions in the /usr/lib directory by entering **chmod 755 -R mono**.
 d. At the command prompt, enter **cd /etc**.
 e. Change the Mono permissions in the /etc directory by entering **chmod 755 -R mono**.
3. Open YaST by selecting the **YaST** icon (on your desktop); then enter the ***root password***.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The Yast Control Center appears.

4. From the left, select **Network Services**; from the right, scroll down and select one of the following:

 - **iFolder 3.x**

 or

 - **iFolder 3.x Web Access**

 After a few moments, a message appears indicating that the RPMs for the selected service are not installed.

5. Continue by selecting **Continue**.

 A message appears asking for a Novell OES Linux CD.

6. Insert the requested CD; then select **OK**.

 After the packages are installed and configured, the configuration pages for Novell iFolder 3.*x* or Novell iFolder 3.*x* Web Access are displayed.

7. Remove the CD from the CD drive.

Although this method only allows you to install one iFolder service at a time, you can immediately configure the service without starting a separate configuration process.

How to Configure the iFolder Enterprise Server

After you install the iFolder enterprise server, you must configure the iFolder services, including the LDAP, iFolder system, and iFolder administration settings.



If you install iFolder when you install OES Linux, the same parameters described in this procedure are available as an integrated part of the server installation.

However, you cannot choose an NSS volume as the iFolder System Store Path because NSS volumes cannot be created during the server platform installation.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Do the following:

1. If you plan to use an NSS volume as the System Store Path for the users' iFolder data, use iManager to create the NSS volume; then create a directory on the volume.
2. From the OES Linux server desktop, open YaST by selecting the **YaST** icon (on the desktop); then enter the ***root password***.

 The Yast Control Center appears.
3. From the left, select **Network Services**; from the right, scroll down and select **iFolder 3.x**.
4. (Conditional) If a warning message appears indicating that you have already configured iFolder 3.*x*, continue by selecting **Yes**.

 After a few moments, a Novell iFolder 3 LDAP server Configuration page appears:

Figure 8-4



Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Configure the LDAP server using the following guidelines:

- **Local or Remote Directory Server.** Select **Local system** if your LDAP directory services are running on the same server as the iFolder 3 enterprise server. Otherwise, select **Remote system**.
- **Directory Server Address.** If directory services are Remote, specify the IP address of the LDAP server to use for this iFolder enterprise server.
- **LDAP Admin Name.** This is the fully distinguished name of the Admin user with administrative rights to LDAP.

 This information is needed during the configuration to create User objects for the administrative iFolder Proxy user. The LDAP schema is not extended.

 Enter an existing username and an existing context. If the user does not already exist, the username is created only if the context is valid.

 For example:

 cn=admin.o=acme
- **LDAP Admin Password.** Enter the LDAP Admin user's password.
- **iFolder User Login Based on Which LDAP Attribute.** Enter which LDAP attribute of the User account to apply when authenticating users.

 Each user enters a Username in this specified format at login time. Options are Common Name (cn, default) and e-mail address (mail).

 For example, if a user named John Smith has a common name of jsmith and email of john.smith@example.com, this field determines whether the user enters jsmith or john.smith@example.com as the Username when logging in to the iFolder server.

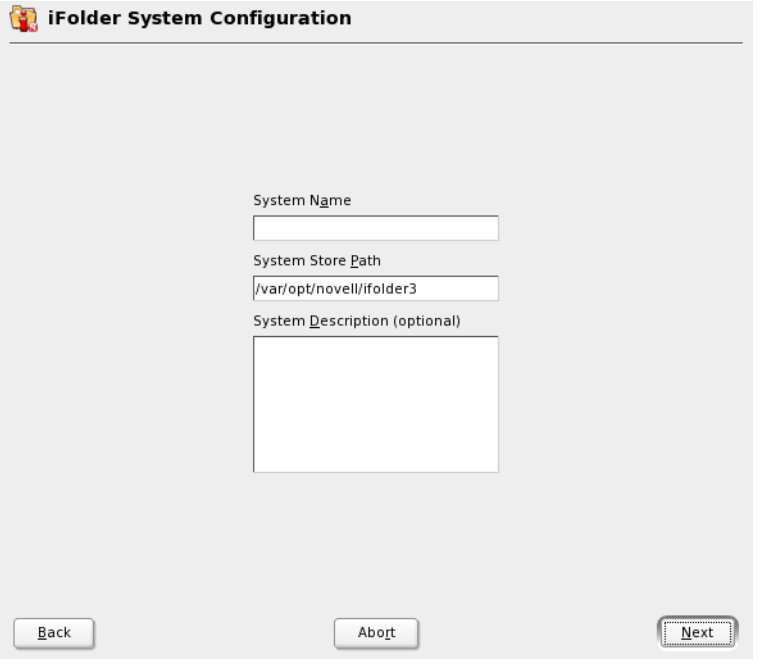
 This setting cannot be changed after the installation.

5. When you finish, continue by selecting **Next**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

YaST verifies the user credentials, and then displays an iFolder System Configuration page:

Figure 8-5



Configure the iFolder system using the following guidelines:

- **System Name.** A unique name to identify your iFolder 3 server (such as **IF3EAST Server**).
- **System Store Path.** The case-sensitive location where this iFolder enterprise server stores the iFolder 3.*x* application files and the users' iFolders and files.

 This location cannot be modified after the initial configuration.

 The store path should not be set at the root of a volume, such as the root (/) or the root of a mount point (for example, /mnt/ifolder3).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Make sure to add a standard directory to the end of the path. For example,

/var/opt/novell/ifolder3/data

/ifolder3/data

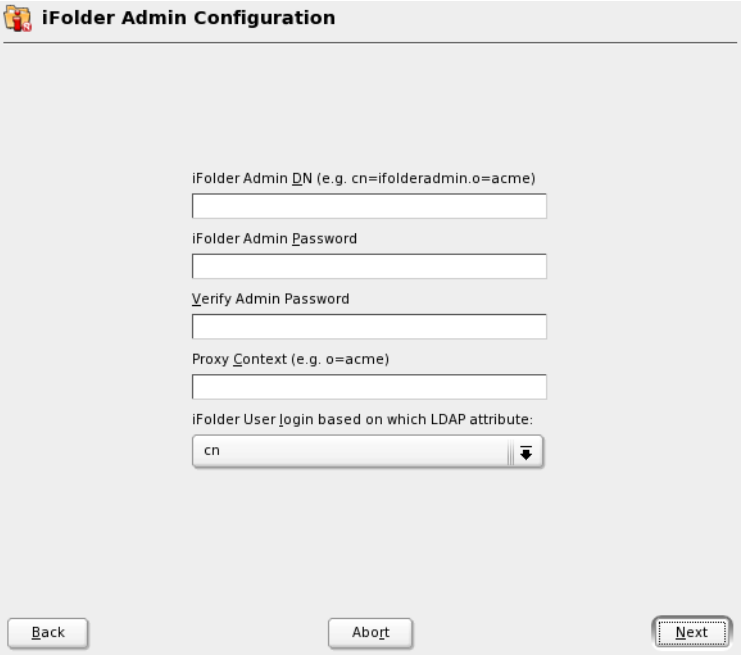
/mnt/ifolder3/data

- **System Description.** A descriptive label for your iFolder 3 server (such as **iFolder 3 Eastern Server**).

6. When you finish, continue by selecting **Next**.

 An iFolder Admin Configuration page appears:

Figure 8-6



Configure the iFolder Admin account using the following guidelines:

- **iFolder Admin DN.** You use the iFolder Admin user to manage iFolder services with the iManager iFolder 3 plug-in.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If this user does not already exist, it is created and granted the necessary rights to manage all iFolder services.

Specify the fully distinguished name of the iFolder admin user, such as

cn=ifolderadmin.o=acme

- **iFolder Admin User Password.** This is the password to use for the iFolder admin user. Type the password again to verify the entry.
- **Proxy Context.** This is the existing context where you want to create the iFolder Proxy user.

 A generated username and password are used to create the user in the specified context, and then the user is granted the Read right to LDAP.

 The generated username is iFolderProxy*xxxx*, where *xxxx* is a 4-digit random number.

 You should never have to modify the user and password for the iFolder Proxy user, but it is possible.

7. When you finish, continue by selecting **Next**.

 YaST configures iFolder 3.*x*, and then asks if you want to restart Apache.

8. Restart Apache by selecting **Yes**.

 YaST activates the iFolder service and you are returned to the YaST Control Center.

 However, you still need to restart Apache and Tomcat manually for access to web pages (such as the server home page).

9. Restart Apache and Tomcat from a terminal window by entering the following commands (in the order listed):

 rcapache2 stop
 rcnovell-tomcat4 stop
 rcnovell-tomcat4 restart
 rcapache2 start

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



If you ever need to run the configuration again, you can modify any field except the System Store Path and the iFolder User Login Based on Which LDAP Attribute options. These parameter settings cannot be modified after the initial configuration.

How to Configure the iFolder Web Access Server

After you install the iFolder Web Access server, you must indicate which iFolder enterprise server it supports and the user-friendly URL that users enter in their Web browsers to access it.

Do the following:

1. From the OES Linux server desktop, open YaST by selecting the **YaST** icon (on the desktop); then enter the ***root password***.

 The Yast Control Center appears.

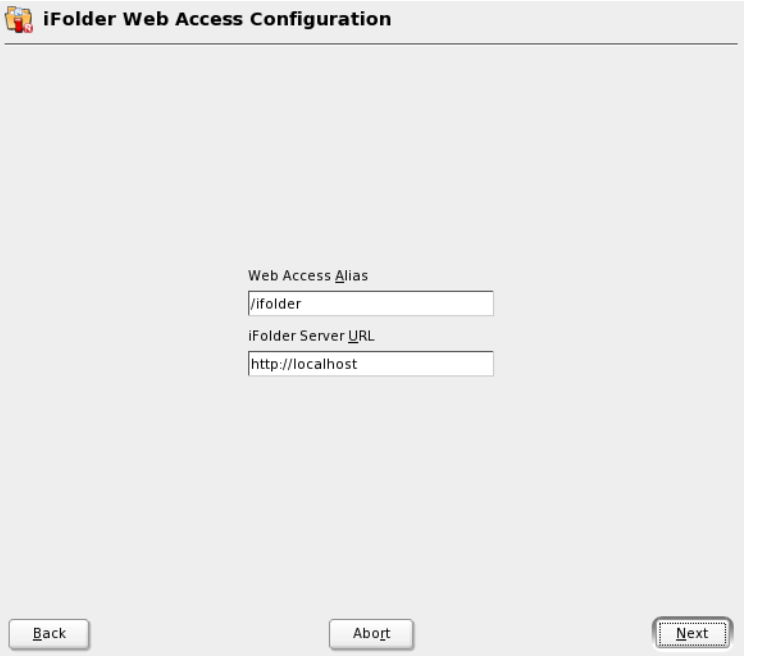
2. From the left, select **Network Services**; from the right, scroll down and select **iFolder 3.x Web Access**.

3. (Conditional) If a warning message appears indicating that you have already configured iFolder 3.*x* Web Access, continue by selecting **Yes**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

An iFolder Web Access Configuration page appears:

Figure 8-7



Configure the iFolder Admin account using the following guidelines:

- **Web Access Alias.** This is the user-friendly path for accessing iFolder services on the specified iFolder 3 enterprise server (such as **/ifolder**).
- **iFolder Server URL.** The iFolder 3 Web Access server and the iFolder 3 enterprise server can reside on the same computer or on different computers.

 Enter the URL and port number of the iFolder 3 enterprise server served by this instance of Web Access.

 Make sure to specify secure HTTP (https://) in the URL for secure communications between the enterprise server and the Web Access server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

HTTPS (SSL) encrypts information transmitted over shared IP networks and the Internet. It helps protect your sensitive information from data interception or tampering.

By default, the iFolder enterprise server is configured to communicate with the iFolder Web Access server via SSL (HTTPS). For most deployments, this setting should not be changed.

If the iFolder deployment is small enough that you can install both the Web Access server and the iFolder enterprise server on the same machine, you can optionally specify HTTP (http://) to use clear traffic, which would increase the performance of local communications between the two servers.

For example, use **https://192.168.1.1:443** (different servers) or **http://localhost:80** (same server).

4. When you finish, continue by selecting **Next**.

 YaST configures iFolder 3.*x* Web Access; then it asks if you want to restart Apache.

 Restarting Apache is necessary to use the new settings.

5. Restart the Apache web server by selecting **Yes**.

 YaST activates the iFolder services and you are returned to the YaST Control Center.

How to Install the Novell iFolder 3 Plug-In for iManager

Before you can manage Novell iFolder 3 services, you must install the iFolder iManager Module for Novell iManager 2.5.

After it is installed, this plug-in is named Novell iFolder 3 in the iManager Roles and Tasks list.

Make sure you meet prerequisites, then use one of the methods for installing the iFolder plug-in:

- Prerequisites

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Installing a Plug-In When RBS Is Not Configured
- Installing a Plug-In When RBS Is Configured

Prerequisites

The following are prerequisites you need to meet before managing iFolder 3.*x* from iManager:

- **iManager 2.5.** If you have not already done so, install Novell iManager 2.5 on the same or different server as your iFolder server.
- **Role-Based Services.** The iFolder 3 plug-in supports the optional use of Role Based Services (RBS) in Novell iManager.

 RBS gives you the ability to assign specific tasks to iManager admin users and to present the admin user with only the tools necessary to perform a specified set of tasks or manage only specified objects as determined by their roles.

 What admin users see when they access iManager is based on their role assignments in Novell eDirectory. Only the roles and tasks assigned to that user are displayed.

Installing a Plug-In When RBS Is Not Configured

If you do not have Role-Based Services (RBS) configured for Novell eDirectory, do the following to install the iFolder Manager Module:

1. From a supported web browser, log in as admin to iManager on the iFolder server where you installed iManager using the following URL:

 https://*ifolder.example.com*/nps/iManager.html

 Replace ***ifolder.example.com*** with the IP address (such as 10.200.200.2) or the DNS name of the iFolder server.

 If you installed iManager on a different server in the same tree as your iFolder server, log in to iManager on that server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. From the toolbar at the top of iManager home page, select the **Configure** icon (person seated behind a desk).
3. From the left (under Roles and Tasks), expand **Module Installation**; then select **Available Novell Plug-In Modules**.
4. Locate the **iFolder 3 iManager Module** plug-in, select its plug-in check box; then select **Install**.

 The installation can take a few minutes. You should receive a message confirming a successful installation.
5. Close the message by selecting **OK**; then exit iManager and close the web browser window.
6. Stop and start the Tomcat servlet engine by entering the following command at a terminal window command prompt:

 rcnovell-tomcat4 restart

 Tomcat sometimes requires several minutes to fully initialize. Wait at least five minutes before trying to log in to iManager.
7. Verify that the plug-in is enabled by opening iManager in a web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of Roles and Tasks.

Installing a Plug-In When RBS Is Configured

If you are running iManager in Assigned Mode and have RBS configured for eDirectory, complete the following steps to install the iFolder iManager Module:

1. From a supported web browser, log in as admin to iManager on the iFolder server where you installed iManager using the following URL:

 https://*ifolder.example.com*/nps/iManager.html

 Replace ***ifolder.example.com*** with the IP address (such as 10.200.200.2) or the DNS name of the iFolder server.

 If you installed iManager on a different server in the same tree as your iFolder server, log in to iManager on that server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. From the toolbar at the top of the iManager home page, select the **Configure** icon (person seated behind a desk).
3. From the left (under Roles and Tasks), expand **Module Installation**; then select **Available Novell Plug-In Modules**.
4. Locate the **iFolder 3 iManager Module** plug-in, select its plug-in check box; then select **Install**.

 The installation can take a few minutes. You should receive a message confirming a successful installation.
5. Close the message by selecting **OK**; then exit iManager and close the web browser window.
6. Stop and start the Tomcat servlet engine by entering the following command at a terminal window command prompt:

 rcnovell-tomcat4 restart

 Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log in to iManager.
7. After Tomcat initializes, from a web browser, log in to iManager as a **Collection Owner** (such as admin).
8. Select the **Configure** icon.
9. On the left under Role-Based Services, select **RBS Configuration**.

 The table on the Collections tabbed page displays modules ready to update.
10. Locate the collection where you want to install the plug-in; then select its **Out-of-Date** number.

 The iFolder iManager Module plug-in should be displayed under Modules Not Yet Installed column.
11. Select the **iFolder iManager Module** plug-in; then select **Update**.
12. Wait for the Completed message; then continue by selecting **OK**.
13. Verify that the plug-in is enabled by opening iManager in a web browser and checking to see if the Novell iFolder 3 plug-in appears in the list of Roles and Tasks.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



To re-install an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory, using the Module Configuration > Delete RBS Module task.

How to Access iManager and the Novell iFolder 3 Plug-In

The Novell iFolder 3 plug-in to Novell iManager 2.5 is the tool used to manage your iFolder server.

To access the Novell iFolder plug-in from iManager, do the following:

1. From a supported web browser, log in as admin to iManager on the iFolder server where you installed iManager using the following URL:

 https://*servername.example.com*/nps/iManager.html

 Replace ***servername.example.com*** with the IP address (such as 10.200.200.2) or the DNS name of the OES Linux server where you installed iManager.

 This might be the same computer on which you installed iFolder 3.*x* or iFolder 3.*x* Web Access, or it might be a different computer.

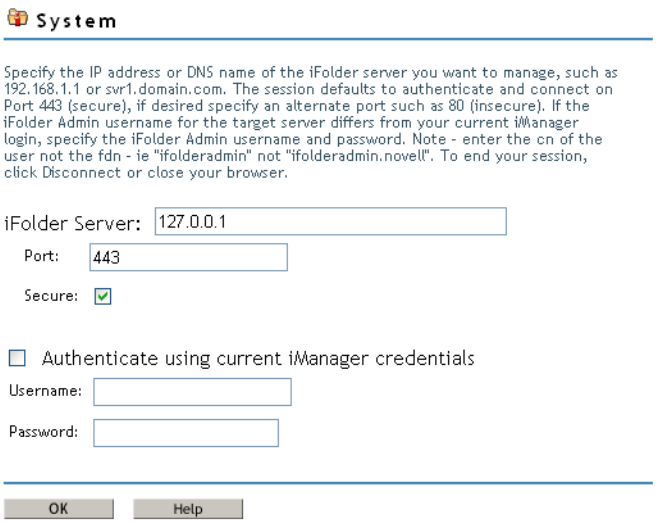
2. From the iManager login page, enter the Admin ***username*** and ***password*** you created during the OES Linux server installation; then select **Login**.

3. From the left (under Roles and Tasks), expand **Novell iFolder 3**; then select **System**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A connect login page appears for the System task:

Figure 8-8



This connect login page appears the first time you select any of the Novell iFolder 3 tasks during an iManager session.

After logging in once, you do not have to log in again for any of the other Novell iFolder 3 tasks.

The following describes the login options:

- **iFolder Server.** Enter the DNS name or IP address of the iFolder enterprise server you want to manage (such as **svr1.example.com** or **192.168.1.1**).
- **Port and Secure.** Enter the port to use for your management session and indicate whether the port traffic is secure (select Secure) or insecure (deselect Secure).

 The default setting is Port 443 for secure traffic.
- **Authenticate using current iManager credentials.** If you logged in to iManager with the same username as the iFolder Admin user of the target server, select **Authenticate using current iManager credentials**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Username and Password.** If you logged in to iManager with a different username than the iFolder Admin user of the target server, make sure Authenticate using current iManager credentials is deselected, and then enter the iFolder Admin ***username*** and **password**.

4. Connect to the iFolder server by selecting **OK**.
5. (Conditional) If prompted to accept the server's certificate, review the certificate information, and then accept the certificate by selecting **OK**.

 Novell iFolder 3.*x* opens to the System Management page, which consists of a tabbed list of the main administrative iFolder functions that you can perform.
6. When you are done managing the iFolder server, select **Disconnect** (located in the upper right corner) or close your web browser to disconnect from the iFolder server you are managing.

 If you do not log out, the connection to the iFolder enterprise server remains open until your session times out, which can be a security risk.

How to Provision Users and iFolder Services

After you configure your Novell iFolder 3.*x* enterprise server, you must specify containers and groups as Search DNs in the LDAP settings. iFolder uses these to provision user accounts.

The contexts you plan to use as Search DNs in the LDAP settings must exist in the LDAP directory; they are not created and configured from within the iFolder plug-in.

Do the following:

- Configure the Search DNs for Provisioning Users
- Synchronize the List of Provisioned Users with the LDAP Directory

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Configure the Search DNs for Provisioning Users

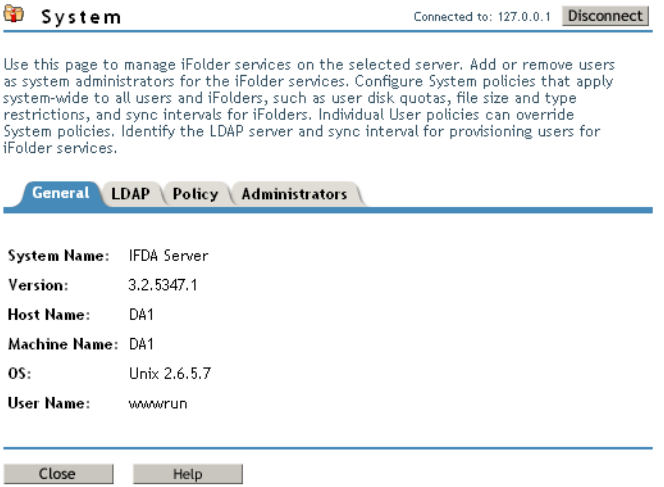
All users in the containers and groups listed in the iFolder LDAP settings' Search DN field are automatically provisioned as iFolder users.

To configure the search DNs for provisioning users, do the following:

1. From iManager on the left, expand **Novell iFolder 3**; then select **System**.
2. (Conditional) If an iFolder connect login page appears, log in as the iFolder admin user (see "How to Access iManager and the Novell iFolder 3 Plug-In" on 8-55).

 A System page appears:

Figure 8-9



3. Select the **LDAP** tab.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

An LDAP tab page appears:

Figure 8-10

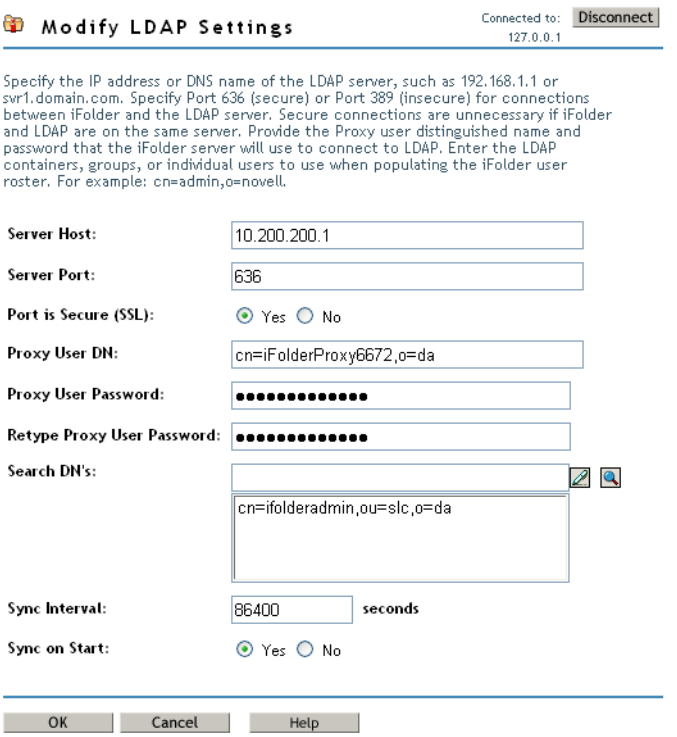


4. From the bottom of the page, select **Modify**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

A Modify LDAP Settings page appears:

Figure 8-11



5. Repeat the following for each context you want to add or modify:

 a. Specify the context:

 - **Add.** Type the ***DN*** of the LDAP context you want to add in the Search DN's field.
 - **Search.** To search, select the **Search** icon (magnifying glass) to open a browsable list of LDAP objects; then select the ***context*** to add.

 The LDAP object selector is not available if you logged in to iManager in a different LDAP tree than the one where the Server Host (iFolder's LDAP server) resides.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Edit.** To edit a value, select it from the list of Search DNs and select the **Edit** icon (pen); then make your changes.

 DNs are entered in LDAP format, such as

  ```
  o=acme
  ```

  ```
  ou=group,o=acme
  ```

 The iFolder Admin user created and configured during installation. It is tracked by its GUID, so it is available even if the Search DN is empty, or if you specify Search DNs that do not contain the Folder Admin user.

 This identity must be provisioned to enable the iFolder Admin to perform management tasks.

b. When you finish, apply the change by selecting **OK**.

6. Continue with "Synchronize the List of Provisioned Users with the LDAP Directory" on 8-61.

Synchronize the List of Provisioned Users with the LDAP Directory

To synchronize the list of provisioned users with the LDAP directory, do the following:

1. From iManager on the left, expand **Novell iFolder 3**; then select **System**.
2. (Conditional) If an iFolder connect login page appears, log in as the iFolder admin user (see "How to Access iManager and the Novell iFolder 3 Plug-In" on 8-55).

 A System page appears.
3. Select the **LDAP** tab.

 An LDAP tab page appears.
4. From the bottom of the page, select **Update and Synchronize Now**.

 Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

During LDAP synchronization, the iFolder server queries the LDAP server to retrieve a list of users in the DNs as specified in the Search DN field.

This might take several minutes, depending on the size of your LDAP directory.

5. When the synchronization is complete, from the top of the page select **Disconnect**; then close iManager.

The iFolder User list is updated periodically based on the LDAP synchronization interval.

Whenever you remove users from an LDAP Search DN or remove contexts from the Search DN list, you should synchronize the list immediately using “Update and Synchronize now” to enforce your changes.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise 8-1 Install and Configure iFolder 3.2 on the DA1 Linux Server

As network administrator for Digital Airlines, you have received requests from management and employees to provide a personal file storage service.

You decide that iFolder meets all the requirements, and want to implement the 3.2 version (included in Novell OES SP2) to take advantage of the new features.

In this exercise, you start the process by performing the following tasks:

- Install and configure iFolder 3.*x* on the DA1 Linux server.
- Install the iManager iFolder plug-in.
- Install and configure iFolder 3.x Web Access on the DA1 Linux server.
- Provision Digital Airlines employees' user accounts to access iFolder.

Exercise 8-1 Install and Configure iFolder 3.2 on the DA1 Linux Server is in your *Integrating Novell Open Enterprise Server for Linux Workbook* on page 8-2.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 4 Manage iFolder 3.*x* as an Administrator

Once you have installed iFolder 3.*x* and provisioned users, you are ready to begin managing iFolder.

The following are some basic tasks you need to know how to do to manage iFolder 3.*x* as an administrator on an OES Linux server:

- Distribute and Install the iFolder Client
- Start, Stop, and Restart the iFolder Services
- Manage the Simias Log and Simias Access Log
- Recover Individual Files or Directories
- Configure System Policies
- Modify the iFolder LDAP Settings
- Manage the iFolder Web Access Server
- Configure iFolder Users
- Manage iFolders



For additional information on managing iFolder 3.*x* as an administrator, see the *Novell iFolder Administration Guide for Novell iFolder 3.x* (admin.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Distribute and Install the iFolder Client

After you configure iFolder services on the enterprise server, users can download the installation files for the iFolder client from the iFolder 3.*x* Welcome page.

To know how to manage the distribution of the iFolder 3.*x* client, you need to know how to do the following:

- Check Prerequisites and Guidelines

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Configure the iFolder 3.x Welcome Page
- Download the iFolder Client from the iFolder 3.x Welcome Page
- Install the iFolder Client on Windows 2000/XP/2003



For additional information on distributing and installing the Novell iFolder Client, see the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf) and the *Novell iFolder Administration Guide for Novell iFolder 3.x* (admin.pdf).

You can access these guides from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Check Prerequisites and Guidelines

To use iFolder, your workstation must meet the prerequisites discussed in the following:

- Hardware
- Client Computers
- Mono
- Web Browser
- Network Connection
- Enterprise Server
- Web Access Server

Hardware

The iFolder client requires the following minimum hardware:

- For each workstation:
 - At least enough space on your hard drive to download and install the iFolder client for your system
 - A network adapter

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- A network connection
- When working with a Novell iFolder 3.*x* enterprise server, workstations can use static or dynamic IP addresses

Client Computers

The iFolder client supports the following workstation operating systems:

- Novell Linux Desktop 9 and SUSE Linux Enterprise Desktop 10 (requires the Mono framework)

 The Mono modules you need for this release are included in the iFolder install file.

- Windows 2000/XP/2003 with the latest Microsoft .NET 1.1 support patches

 Make sure you have installed the latest critical updates for your operating system and for .NET 1.1. See the Windows Update Web site (http://windowsupdate.microsoft.com).

- Macintosh OS X v10.3 and later (requires the Mono framework)

 The Mono modules you need for this release are included in the iFolder install file.

Mono

For a Linux or Macintosh workstation, the iFolder client requires the Mono framework.

Mono is a development platform for running and developing modern applications. Based on the ECMA/ISO standards, Mono can run existing programs that target the .NET or Java frameworks.



The Mono Project is an open source effort led by Novell and is the foundation for many new applications. For information about Mono, see the Mono Project web site at http://www.mono-project.com.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

When you install the iFolder client for Linux and Macintosh, you must also install Mono as a dependent application for iFolder. The required version of Mono is packaged in the iFolder client installation file that you download from the iFolder server.

The following table lists the versions of Mono used in the different iFolder releases on Linux and Macintosh:

Table 8-6

iFolder Client Version	Mono Version
iFolder client for Novell iFolder 3.0 (released for OES Linux)	■ For Linux: 1.1.7.1.44342 ■ For Macintosh: 1.1.7.2
iFolder client for Novell iFolder 3.1 (released for OES SP1 Linux) and 3.2 (released for OES SP2 Linux)	■ For Linux: 1.1.7.7 ■ For Macintosh: 1.1.7.7*x*

Make sure to use the required version of Mono. If you have a different version of Mono on your Linux or Macintosh computer, uninstall it before you install iFolder and the required version of Mono.



The iFolder client for Linux or Macintosh supports only the version of Mono included in the installation software.

If you need to upgrade Mono for another reason, please check the iFolder 3.*x* online documentation to see if Novell explicitly supports that Mono version and to learn any necessary steps to make the upgrade work correctly.

For information, see the latest version of the iFolder 3.*x* Readme on the Novell iFolder 3.*x* Documentation web site at http://www.novell.com/documentation/ifolder3.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Web Browser

You need one of the following supported web browsers on your client computers:

- Mozilla Firefox
- Microsoft Internet Explorer
- Safari (on Macintosh)

Novell iFolder 3.*x* servers expect users to connect to the enterprise server account and the web access server with SSL 3.0 connections. Both the client and browser connections use the browser's settings for SSL.

If Microsoft Internet Explorer is installed on your system, the iFolder client uses those settings over any other browser configuration for the client.

Make sure the Internet Explorer browser settings and other browsers you use to connect to iFolder servers are configured to use SSL 3.0.

Network Connection

An active network connection is necessary to synchronize files in your iFolders. Your computer must be active and online for access to and synchronization with any enterprise servers where you have iFolder accounts.

Enterprise Server

Users will need the server IP address or DNS name (such as 10.200.200.1 or da1.da.com) of the Novell iFolder 3.*x* enterprise server for their iFolder accounts.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Web Access Server

Users will also need the URL with the server IP address or DNS name (such as http://10.200.200.1/ifolder or http://da1.da.com/ifolder) of the Novell iFolder 3.*x* Web Access server for their iFolder account.

Configure the iFolder 3.*x* Welcome Page

The iFolder 3.x enterprise server installs the client install files in the /var/opt/novell/tomcat4/webapps/ifolder3-client/ directory. The references to these files are in the /var/opt/novell/tomcat4/webapps/welcome/WEB-INF/XMLData/ifolder3.xml file.

After the iFolder 3.*x* enterprise server installation is complete, you must restart Tomcat 4 to install the iFolder 3.*x* from the OES Welcome pages.

You can stop and start the Tomcat servlet engine by entering the following commands at the server console:

```
rcnovell-tomcat4 stop
rcnovell-tomcat4 start
```

Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to access the OES Welcome pages.

Download the iFolder Client from the iFolder 3.*x* Welcome Page

You can download the iFolder client from the iFolder 3.*x* Welcome page by doing the following:

1. From a supported web browser, display the iFolder 3.*x* Welcome page using the following URL:

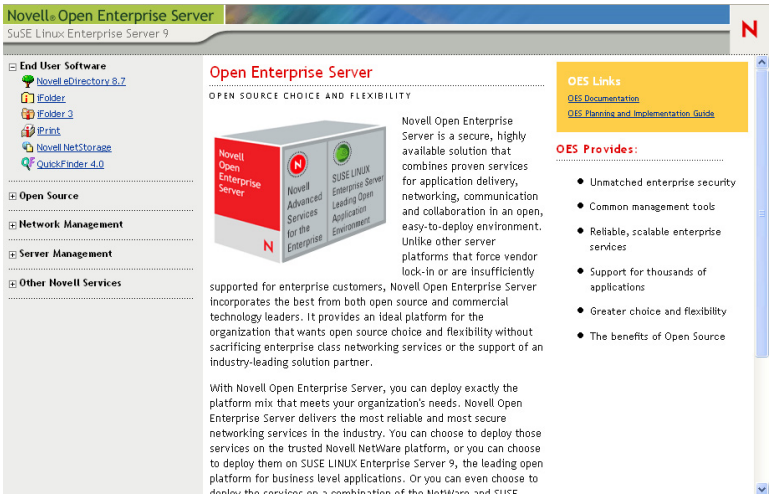
 http://*ifolder3.example.com*

 Replace ***ifolder3.example.com*** with the DNS name or the IP address (such as 10.200.200.1) of the OES Linux server where the Novell iFolder 3.*x* enterprise server is installed.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A Novell Open Enterprise Server Welcome page appears:

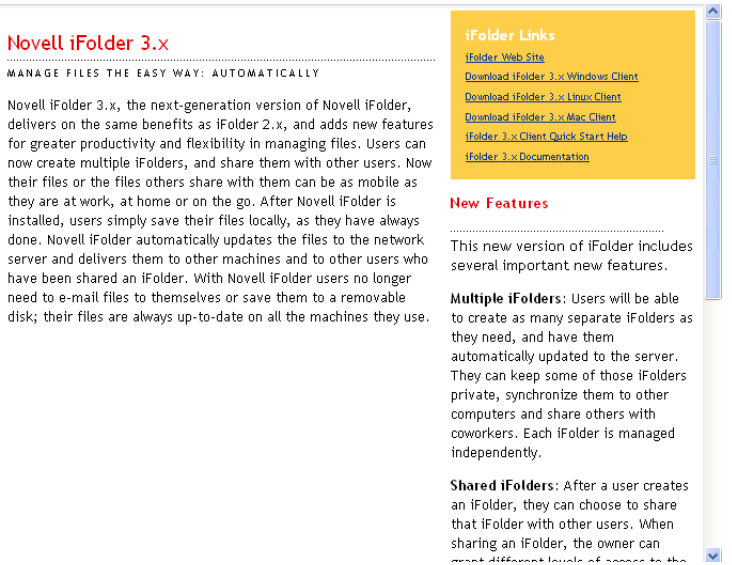
Figure 8-12



2. From the left under End User Software, open the iFolder 3.*x* Welcome page by selecting **iFolder 3**.

 The iFolder 3.*x* Welcome page appears (on the right):

Figure 8-13



Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

From the yellow box in the upper left corner of the page, select one of the following client links to download the installation files for the iFolder client for Novell iFolder 3.*x*:

Table 8-7

Link Name	Operating System and File Name
iFolder 3.*x* Windows Client	■ Windows 2000/XP/2003 ifolder3-windows.exe
iFolder 3.*x* Linux Client	■ Novell Linux Desktop 9 and later (including SLED 10) ifolder3-linux.tar.gz
iFolder 3.*x* Mac Client	■ Macintosh OS X v10.3 and later ifolder3-mac.tar.gz

After expanding the tar.gz files, you are ready to install the iFolder client and its dependencies with the following files:

Table 8-8

iFolder Client	Install Files
iFolder for Windows	ifolder3-windows.exe
iFolder for Linux	../linux/ifolder3 directory ifolder3-3.x.*yyyymmdd*-1.i686.rpm nautilus-ifolder-3.x.*yyyymmdd*-1.i586.rpm simias-1.0.*yyyymmdd*-1.i686.rpm ../linux/mono directory gtk-sharp-1.0.9-0.sles9.novell.i586.rpm libgdiplus-1.1.7-1.ximian.i586.rpm mono-core-1.1.7.x-*xxxxx-x*.novell.i586.rpm mono-data-1.1.7..x-*xxxxx-x*.novell.i586.rpm mono-web-1.1.7..x-*xxxxx-x*.novell.i586.rpm xsp-1.0.9-0.novell.noarch.rpm
iFolder for Mac	ifolder3-3.x.*yyyymmdd*.dmg MonoFramework-1.1.7..*x-x*.dmg

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Install the iFolder Client on Windows 2000/XP/2003

In this course, you install the iFolder client on a Windows workstation (XP Professional) and run the iFolder client from a SUSE Linux Enterprise Desktop 10 (SLED 10) workstation.

The iFolder client is already installed on SLED 10.



For details on installing the iFolder 3.*x* client on Novell Linux Desktop 9 and Macintosh, see "Installing the iFolder Client" on page 33 of the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

To install the iFolder client on Windows, do the following:

1. Log on to the computer as an **Administrator** user (or equivalent user).
2. Save the **iFolder.exe** file to a local directory.
3. Install iFolder by double-clicking the file; then follow the on-screen instructions.

 iFolder for Windows requires the Microsoft .NET framework. If .NET is not detected, the installation automatically downloads and installs .NET.
4. When prompted to reboot the computer, do one of the following:
 - Select **OK** and allow the reboot to continue; then continue with Step 5.
 - Select **Cancel** and log off as the Administrator user (or equivalent user) identity; then continue with Step 5.
 - If you want to create an iFolder account from your current login, select **Cancel** and start iFolder by selecting **Start > Programs > iFolder 3 > iFolder 3 Client**; then continue with Step 6.
5. To run iFolder, log on to the computer with the user identity you want to use when you create iFolders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

iFolder begins automatically whenever you log on to your computer and prompts you to create an iFolder account.

If it does not start, you can start it manually by selecting **Start > Programs > iFolder 3 > iFolder 3 Client**.

If you are running personal firewall software on your computer, you might receive a message asking whether you want to block Mono-XSP.

6. Unblock (or do not block) **Mono-XSP**.

 You are now ready to create an iFolder account.

Start, Stop, and Restart the iFolder Services

iFolder services start whenever you reboot the system or whenever you start Apache services. As a root user, you can start the Apache services by entering the following command:

/etc/init.d/apache2 start

or

rcapache2 start

iFolder services stop whenever you stop the system or whenever you stop Apache services. As a root user, you can stop the Apache services by entering the following command:

/etc/init.d/apache2 stop

or

rcapache2 stop

If you need to restart iFolder services, you must stop and start Apache services. Avoid using the Apache restart command (such as rcapache2 restart).

CNI USE ONLY-1 HARDCOPY PERMITTED

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If any other modules using the Apache instance do not exit immediately in response to the Apache restart command, iFolder might hang.

Manage the Simias Log and Simias Access Log

On the iFolder enterprise server, the following two logs track events:

- **Simias Log.** The /simias/Simias.log file contains status messages about the health of the Simias Service.
- **Simias Access Log.** The /simias/Simias.access.log file contains file access events for data and metadata about iFolders, users, membership in shared iFolders, and so on.

 It reports the success of the event and identifies who did what and when they did it.

 For example, if a file was deleted on the server, it identifies the user who initiated the deletion.

Review the logs whenever you need to troubleshoot problems with your iFolder system. The Simias Log4net file (/simias/Simias.log4net) allows you specify output location of the log files and what events are recorded at run time.

Its parameters are based on, but not compliant with, the Apache Logging Services (http://logging.apache.org/log4net).



For a list of modifiable parameters, see "Managing the Simias Log and Simias Access Log" on page 68 of the *Novell iFolder Administration Guide for Novell iFolder 3.x* (admin.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Recover Individual Files or Directories

To recover individual files or directories for a user from the Simias data collections, do the following:

1. Collect information that uniquely identifies the file or directory to be recovered, such as a combination of the following:
 - iFolder name, such as MyiFolder
 - iFolder owner
 - iFolder member list
 - Relative path of the file or directory, such as /MyDir1/MyDir2/myfile.txt
 - Time stamp or approximate time of the version desired
 - Other files or directories in the iFolder
2. Log in to iManager with the Admin ***username*** and **password**.
3. Under Roles and Tasks, expand **Novell iFolder 3**; then select **iFolders**.
4. If prompted, connect to the iFolder server where the iFolder is stored by entering the name of the iFolder server and iFolder Admin ***username*** and ***password***.
5. From the Search for iFolders page, search for the target ***iFolder*** (such as MyiFolder).
6. Under Search Results, select the ***Name*** link of the target iFolder; then note the path to its root directory.

 For example:

   ```
   /var/opt/novell/ifolder3/simias/SimiasFiles/
   62ba1844-6987-47fc-83ab-84bbd5d6130b/MyiFolder
   ```

7. From the iFolder server, use your normal file system restore procedures to restore the target file or directory from backup to a temporary location.

 For example, restore

   ```
   /var/opt/novell/ifolder3/simias/SimiasFiles/
   62ba1844-6987-47fc-83ab-84bbd5d6130b/MyiFolder/
   MyDir1/MyDir2/MyFile
   ```


Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

to

```
/tmp/MyFile
```



Do not restore the file to its original location, or to any location under the Simias store directory.

8. Use one of the following methods to restore the recovered file to the target iFolder:

 - **Via email.** Send the restored files or directory to the iFolder owner or to any member who has the Write right to the iFolder.

 For example, email the recovered file, such as /tmp/MyFile, to the user.

 A user with the Write right can restore the file to an iFolder simply by copying it back to the appropriate location on an iFolder client.

 For example, copy MyFile to /home/username/MyiFolder/MyDir1/MyDir2/MyFile.

 - **Via web access.** Do the following:

 a. In iManager, expand the **Novell iFolder 3** role and select **Folders**.

 b. Search for the ***iFolder*** you want to manage; then select the ***Name*** link for the iFolder.

 c. On the iFolder page, select **Members**; then add yourself as a member of the target iFolder.

 d. From a web browser, log in to iFolder 3.*x* Web Access.

 e. Browse to locate and open the ***iFolder***; then navigate to the directory where the files were originally located, and upload the file to the ***iFolder***.

 For example, upload MyFile to MyiFolder/MyDir1/MyDir2/MyFile.

 If necessary, create the directory you want to restore to, and then upload the files in it.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You can only upload one file at a time, so this option might be viable when only a few files need to be restored.

Configure System Policies

You can use the System Policies page in iManager to manage system-wide policies by doing the following:

- View the Current System Policies
- Modify iFolder System Policies

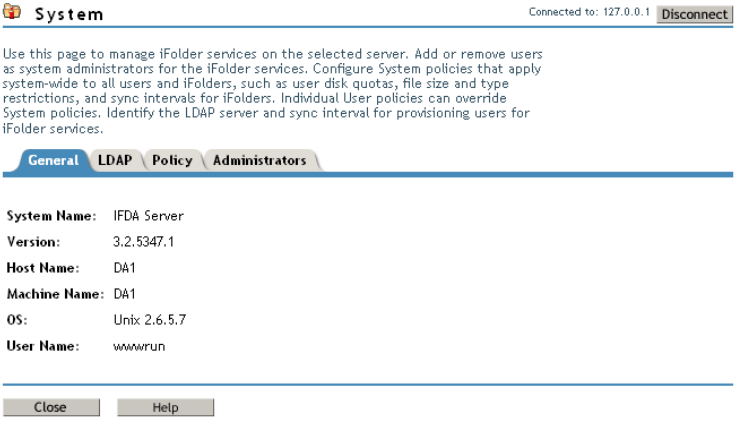
View the Current System Policies

To view the current system policies, do the following:

1. From iManager (on the left), expand the **Novell iFolder 3** role; then select **System**.

 The following appears:

Figure 8-14

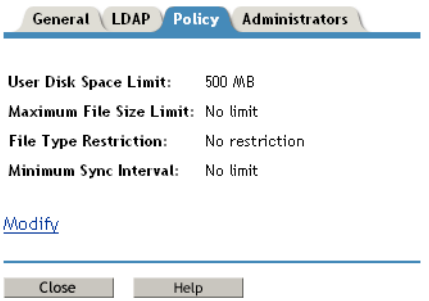


2. Select the **Policy** tab.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-15



The following describes each parameter:

Table 8-9

Parameter	Description
User Disk Space Limit	Specifies the maximum total space that each user's iFolder data is allowed to use, across all iFolders the user owns.
Maximum File Size Limit	Specifies the maximum file size (in MB) that iFolder is allowed to synchronize. If a quota is specified, the effective maximum file size limit is the same as the quota.
File Type Restriction	Specifies a list of file types to include or to exclude from synchronization for all iFolders on the system.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-9**

Parameter	Description
Minimum Synchronization Interval	If this option is enabled, it specifies the minimum interval (in seconds) for synchronizing iFolder data for each user account. Larger values are more restrictive. If the option is disabled, the value is No Limit. The interval timer is reset to the Synchronization Interval value at the end of a synchronization session. When the time elapses, another session is started.

Modify iFolder System Policies

To modify iFolder system policies, do the following:

1. From iManager (on the left), expand the **Novell iFolder 3** role; then select **System**.

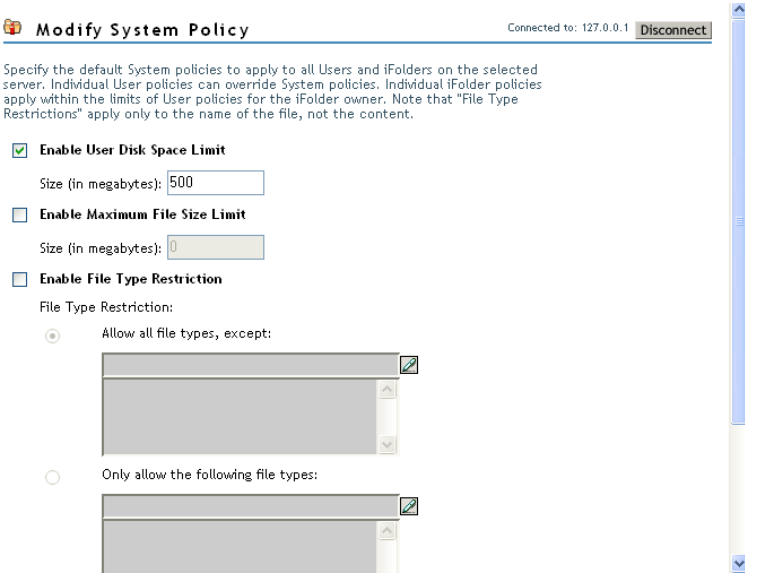
 A System page appears.

2. Select the **Policy** tab; then select **Modify**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-16



3. Enable a policy by selecting a ***check box***; then specify a ***value*** for the policy and apply it by selecting **OK**.

 The following describes each policy:

Table 8-10

Policy	Description
Enable User Disk Space Limit	Deselect the check box to disable a system-wide quota. Select the check box to enable a system-wide quota; then specify the total space quota (in MB) for a user's account. If you enable a system-wide quota that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-10**

Policy	Description
Enable User Disk Space Limit (*continued*)	Enabling or modifying the system-wide quota does not affect existing individual user quotas. Any existing user quota always overrides a system-wide quota, regardless of whether the user quota is lower or higher than the system-wide quota. Default Value: 100 MB
Enable Maximum File Size Limit	Deselect the check box to disable the Maximum File Size Limit policy. If the policy is disabled, the value is reported as No Limit. Select the check box to enable the Maximum File Size Limit policy; then specify the maximum allowed file size in MB. If a quota is specified, the default maximum file size limit is the same as the quota. Consider the following demands on your system to determine an appropriate file size limit for iFolders in your environment: ■ Intended use ■ How often the largest files are modified ■ How the applications that use the largest files actually save changes to the file (whole file or deltas) ■ How frequently the files are synchronized by each member ■ How many users share an iFolder ■ Whether users access iFolder on the local network or across WAN or Internet connections ■ The average and peak available bandwidth

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-10**

Policy	Description
Enable Maximum File Size Limit (*continued*)	Even if you set a very large value as a file size limit and if there is no quota to limit file sizes, the practical limit is governed by the file system on the user's computer. For example, FAT32 volumes have a maximum file size of 4 GB minus 1 byte. Default Value: Disabled, No Limit
Enable File Type Restriction	Specify whether to restrict file types that are synchronized by inclusion or exclusion filters. You cannot set both. Type a file extension, and then select OK to add it to the list. To edit an extension, select the value, select Edit (the pen icon), modify the entry, and then select OK.
Minimum Synchronization Interval	To enable a policy, select the check box, then specify the minimum synchronization interval in seconds. For example, a practical value is 600 seconds (10 minutes). Larger values are more restrictive. To disable the policy, deselect the check box. The value is reported as No Limit. Default Value: Enabled, value=0 seconds.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-10**

Policy	Description
Minimum Synchronization Interval (*continued*)	The effective minimum synchronization interval is always the largest value of the following settings: ■ The system policy (default of zero), unless a user policy is set. If a user policy is set, the user policy overrides the system policy, regardless of whether the user policy is larger or smaller in value. ■ The local machine policy, or the setting on the client machine synchronizing with the server. ■ The iFolder (collection) policy.

Modify the iFolder LDAP Settings

To modify the iFolder LDAP settings, do the following:

1. From iManager (on the left), expand the **Novell iFolder 3** role; then select **System**.

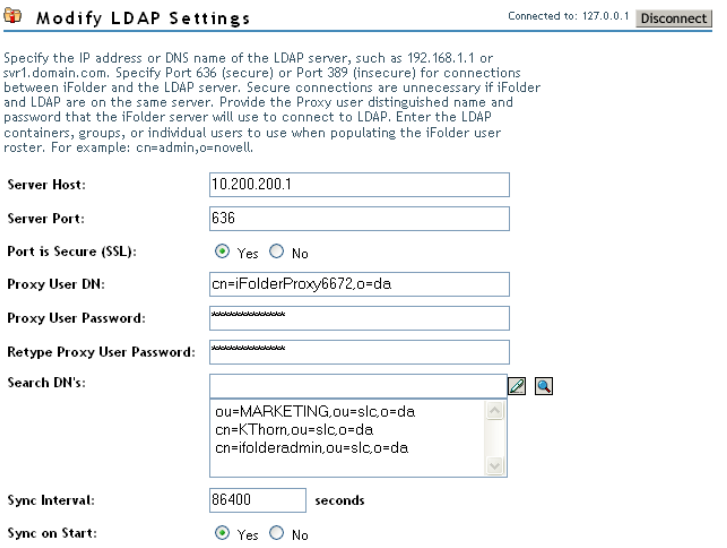
 A System page appears.

2. Select the **LDAP** tab; then select **Modify**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-17



3. Modify a ***field***; then apply the change by selecting **OK**.

The following describes each field:

Table 8-11

Field	Description
Server Host	Specify the DNS name or IP address of the LDAP server. This might be the same or a different server as your iFolder enterprise server or iFolder Web Access server. Make sure this new LDAP server is in the same LDAP tree as the original LDAP server that you specified as Server Host when you configured the iFolder enterprise server in YaST.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-11**

Field	Description
Server Port	Specify port 636 (secure) or port 389 (insecure). If the LDAP server is on the same machine as the iFolder servers, a secure port is unnecessary. Default Value: 636
Port Is Secure (SSL)	Specify whether the iFolder server is configured for SSL exchanges. If SSL is enabled on the server, the value is Yes; otherwise, the value is No. Default Value: Yes
Proxy User DN	The iFolder Proxy user is an existing proxy user identity used to access the LDAP server with Read access to retrieve a list of authorized users. The proxy user is automatically created during the iFolder enterprise server configuration in YaST. The username is autogenerated to be unique on the system. For most deployments, this username should never change. Keep the autogenerated iFolder Proxy username. The iFolder Admin user or equivalent can use the iFolder 3 plug-in for iManager to change the iFolder Proxy user identity in the LDAP settings for the iFolder server. Make sure that the user account assigned as the iFolder Proxy user is different than the one used for the iFolder Admin user and other system users.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-11**

Field	Description
Proxy User DN (*continued*)	Separating the proxy user from the administrator provides privilege separation and is important because the proxy user password is stored in the file system on the iFolder server. Specify the fully distinguished name of an existing user that you want to make the iFolder Proxy user. This identity must have the Read right to the LDAP directory. For example: cn=iFolderProxy1234,o=acme Be sure to also enter the new user's password in the Proxy Password field. After you modify the Proxy user, you might want to immediately synchronize the LDAP user lists using the new iFolder proxy information; otherwise, the Proxy user DN is not tested until the next scheduled synchronization of the user list. Use the Update and Synchronize option on the LDAP Settings page to synchronize the iFolder user list on demand and verify your new Proxy user settings.
Proxy User Password	Specify the password twice, and then select OK to update the password stored in the LDAP Settings. Whenever you modify the Proxy User DN, you must also specify the password associated with the new iFolder Proxy user. The password is used to authenticate the iFolder Proxy user to the LDAP server when iFolder synchronizes users for the iFolder user list.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-11**

Field	Description
Proxy User Password (*continued*)	This password must match the password stored in the iFolder Proxy user's eDirectory object.
Search DN's	Specify the LDAP containers and groups in which iFolder 3.*x* searches for a list of authorized users to provision for iFolder services on this enterprise server. DNs are entered in LDAP format. For example: o=acme ou=group,o=acme To add a DN, type it in the Search DN field, and then select OK. To edit a DN in the list, select it, and then select the Edit icon (pen) to bring it to the Search DN field. Make your changes, and then select OK to accept the changes. To search, select the Search icon (magnifying glass) to open a browsable list of LDAP objects, select the container or group you want to add, and then select OK. The LDAP Object selector is not available if you logged in to iManager in a different LDAP tree than the one where the Server Host (iFolder's LDAP server) resides. To delete a DN from the list, select it, select the Delete icon (red X), and then select OK. When you delete a DN from the Search DNs, users in that DN are removed from the iFolder user list the next time the iFolder server synchronizes LDAP information.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-11**

Field	Description
Search DN's (*continued*)	During LDAP synchronization, the iFolder server queries the LDAP server to retrieve a list of users in the DNs (as specified in the Search DN field). The usernames in the iFolder user list are matched against this official LDAP list. Any new users in the specified Search DNs are added to the iFolder user list. If a user is no longer in the specified DNs, the username is removed from the user list, any iFolders the user owns are orphaned and reassigned to the iFolder Admin user, and the user is removed as a member of other iFolders. The iFolder Admin User is provisioned for services during the installation. It is tracked by its GUID, so it is available even if the Search DN is empty or if you specify Search DNs that do not contain the Folder Admin user. This identity must be provisioned to enable the iFolder Admin to perform management tasks.
Minimum Synchronization Interval	Specify the synchronization interval (in seconds) for the elapsed time to wait between attempts to retrieve an updated list of system users from the LDAP server. Default Value: 86400 seconds (elapsed time of 24 hours from whenever the timer is reset)

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-11**

Field	Description
Synchronization on Start	Specify Yes to immediately synchronize the list of users with the LDAP server when you start the iFolder server, or specify No to wait until the specified Synchronization Interval has elapsed after startup to begin synchronizing. Default Value: Yes

Manage the iFolder Web Access Server

To perform basic iFolder 3.*x* Web Access server administrative tasks, you need to know how to do the following:

- **Start iFolder Web Access services.** iFolder Web Access services start whenever you reboot the system or whenever you start Apache services.

 As a root user, you can start Apache 2 by entering the following:

 /etc/init.d/apache2 start

 or

 rcapache2 start

- **Stop iFolder Web Access services.** iFolder services stop whenever you stop the system or whenever you stop Apache services.

 As a root user, you can stop Apache 2 by entering the following:

 /etc/init.d/apache2 stop

 or

 rcapache2 stop

- **Distribute the Web Access server URL to users.** After you install and configure the iFolder Web Access server, distribute the URL of the server Login page to users.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The URL is the server IP address or DNS name of the Novell iFolder 3.*x* Web Access server for the users' iFolder account (such as http://10.200.200.1/ifolder or http://da1.da.com/ifolder).

- **Configure the HTTP runtime parameters.** Two HTTP runtime parameters—Execution Time-Out (executionTimeout) and Maximum Request Length (maxRequestLength)—can affect the successful upload of a file to the Web Access server.

 The following describes the run time parameters and their default values:

Table 8-12

Parameter	Description
executionTimeout	The interval of time in seconds to wait between the command to upload a file and the successful execution where the file is stored on the iFolder enterprise server. The default time out is 3 minutes. Default Value: 180 (in seconds)
maxRequestLength	The maximum file size in bytes that a user is allowed to upload to the server via the Web Access server. The default maximum size is 10 MB for Web access. This maximum is a software hard limit. You can modify the maximum length for any value up to 10 MB. Default Value: 10240 (in KB)

Using Web Access, a user can upload a local file to the user's iFolder on the enterprise server.

If the file does not upload successfully before the interval times out or if the file size exceeds the allowed maximum, the upload is stopped and reported as a failure.

Because the web browser is controlling the errors, a problem of timing out or exceeding the maximum size might result in a Bad Request or other generic error.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The Execution Time-Out and Maximum Request Length parameters must be configured with compatible settings in the /opt/novell/ifolder3/web/web.config file for the iFolder enterprise server and in the /opt/novell/ifolder3/webaccess /Web.config file for the Web Access server.

The settings in Web.config for the enterprise server must be the same size or larger than the settings in ../webaccess/Web.config for the Web Access server.

For example, the following code is the httpRuntime element with the default settings in the ../webaccess/Web.config file for Web Access:

```
<httpRuntime
    executionTimeout="180"
    maxRequestLength="10240"
/>
```

To modify the httpRuntime parameters, do the following:

1. Stop **iFolder**.
2. Set the httpRuntime parameters on the iFolder Web Access server by editing the values in the **/opt/novell/ifolder3/webaccess/Web.config** file.
3. If necessary, set the httpRuntime parameters on the iFolder enterprise server by editing the values in the **/opt/novell/ifolder3/web/web.config** file.

 Make sure the values are the same size or larger than those set for the Web Access server.
4. Start **iFolder**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

For example, to set the time-out to 5 minutes (300 seconds) and the maximum file size to 5 megabytes (5120 KB) for the Web Access server, modify its httpRuntime parameter values in the ../webaccess/Web.config file:

```
<httpRuntime
    executionTimeout="300"
    maxRequestLength="5120"
/>
```

If the ../webaccess/Web.config values exceed the values in ../web/web.config for the enterprise server, you must also increase the sizes of runtime parameters in that file.

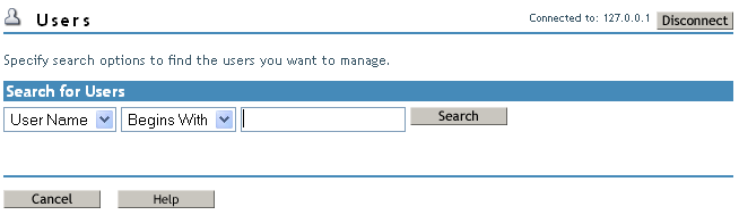
Configure iFolder Users

To configure iFolder users from iManager, do the following:

1. Under iManager Roles and Tasks (on the left), expand the **Novell iFolder 3** role; then select **Users**.

 The following Search page appears:

Figure 8-18



2. Select a ***name criterion*** (User Name, First Name, Last Name).
3. Select a ***filter criterion*** (Contains, Begins With, Ends With, Equals).
4. Use one or more of the following search methods; then select **Search**:
 - Type the name of the user in the Search Users field.
 - Type one or more letters in the Search Users field.

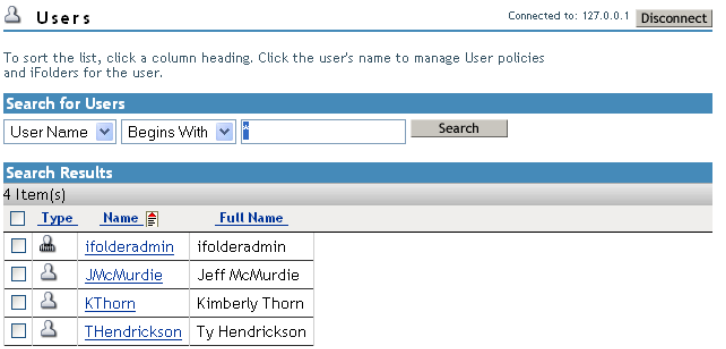
Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Type an asterisk (*) in the Search Users field to return a list of all users on the system.
- Leave the Search Users field empty to return a list of all users on the system.

Do not click anywhere in the page until the page completely refreshes.

A Search Results list similar to the following appears:

Figure 8-19



5. Browse or sort the list of users to locate the one you want to configure.

 Your search results are initially displayed by username in alphabetical order.

 Select the column heading link to initiate the sort with that column as the primary key. Select the same heading link again to initiate a sort in the reverse sort order.

 The following describes each column:

 - **Type.** An icon indicating whether the user has the iFolder Admin right (user wearing a referee-striped uniform) or is a normal user (user icon).
 - **Name.** The username assigned to the user account, such as jsmith.
 - **Full Name.** The first and last name of the user account.

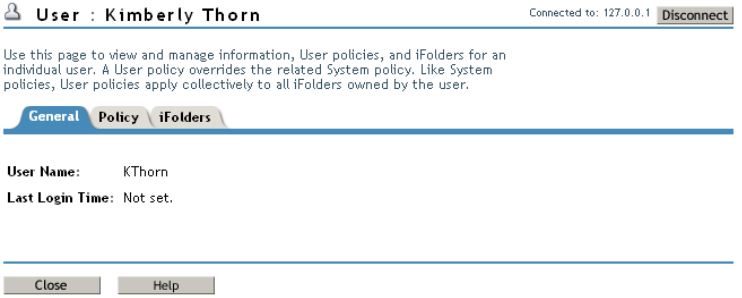
Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Select the user's name to manage User policies and iFolders for the user.

6. View general user account information by selecting the ***Name*** link for the user.

 A page similar to the following appears:

Figure 8-20



 A User page opens to the General tab, which displays the user's full name, username, and the last time the user logged in.

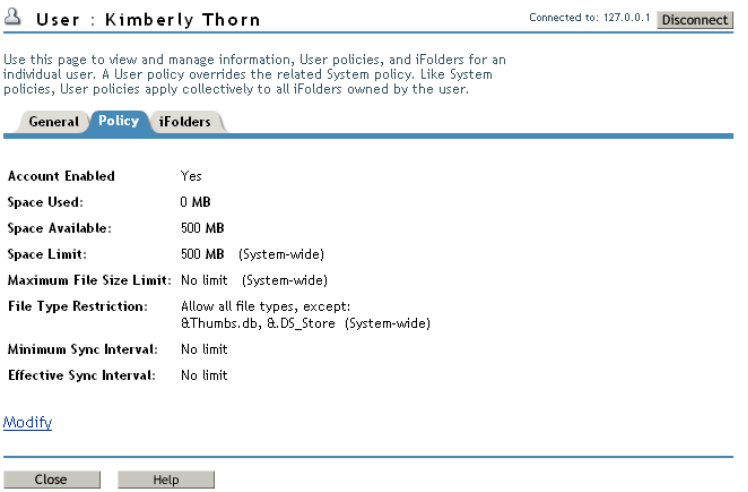
 If the user has not yet set up an account on a client machine, the Last Login Time reports Not Set.

7. Select the **Policy** tab.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following information appears:

Figure 8-21



The following describes each parameter:

Table 8-13

Parameter	Description
Account Enabled	Specifies whether the user is currently allowed to log in to synchronize iFolders.
Space Used	Specifies the total space currently in use on the server for all iFolders owned by this selected user.
Space Available	Specifies the difference between any space restrictions on the account and the space currently in use. If no quota is in effect, the value is No Limit.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-13**

Parameter	Description
Space Limit	Specifies the maximum total space (in MB) that a user's iFolder data is allowed to use, across all iFolders the user owns. A user quota supersedes a system-wide quota, regardless of whether the user quota is larger or smaller than the system-wide quota. The user quota can then be limited, but not increased by a policy on an iFolder. IMPORTANT: Users cannot successfully synchronize files of a size that would cause a quota to be exceeded. If they try to do so, only part of the file is synchronized, resulting in data corruption. If the total space consumed by iFolder data is nearing an effective quota (system, user, or iFolder), the user should stop synchronizing files until one or more of the following tasks results in enough space to safely synchronize the user's files in the iFolder where the file resides: ■ The system-wide quota, user quota for the iFolder owner, and the iFolder quota are modified as needed. ■ Files are moved from any of the iFolders owned by the user to another location where they no longer affect the effective quota, or files are deleted to clear space.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-13**

Parameter	Description
File Type Restriction	Lets you specify whether to allow all file types, or lists the file types to include or to exclude from synchronization for the selected user's account. The file manager files called thumbs.db and .DS_Store are never synchronized. You do not need to keep these files, and synchronizing them results in repeated file conflict errors. If you have not set any individual restrictions for this user, this field reports thumbs.db and .DS_Store as part of the system-wide file-type restrictions. After you set individual file-type restrictions for the user, the user's settings are displayed instead. Even if the thumbs.db and .DS_Store restrictions are not displayed, they always apply; you cannot override them.
Minimum Synchronization Interval	Specifies the minimum interval (in seconds) at which a user's client can check iFolder data on the server and iFolder data on local iFolders to identify files that need to be downloaded or uploaded. Longer interval limits are more restrictive than shorter ones. If a user policy is set, it overrides the system policy, regardless of whether the user's interval is shorter or longer in value.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-13**

Parameter	Description
Effective Synchronization Interval	Specifies the effective minimum synchronization interval for the selected user. The effective minimum synchronization interval is always the largest value specified by the following settings: ■ The system policy (default of zero (0)), unless a user policy is set. If a user policy is set, the user policy overrides the system policy, regardless of whether the user policy is larger or smaller in value. ■ The local machine policy, or the setting on the client machine synchronizing with the server. ■ The iFolder (collection) policy.

8. After viewing the user policy information, you can modify the policy by selecting the **Modify** link.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-22



9. Enable a policy by selecting a ***check box***; then specify a ***value*** for the policy and apply it by selecting **OK**.

 The following describes each policy:

Table 8-14

Policy	Description
Account Enabled	Select the value to enable the account for login. Deselect the value to disable the account for login. If the user is logged in when you make this change, the user's session continues until the user logs out. The policy takes effect the next time the user attempts to log in to the account.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-14**

Policy	Description
Account Enabled (*continued*)	To have the lockout take effect immediately, you must restart the Apache services for the iFolder server; doing so disconnects all active sessions, including the user's session. Default Value: Enabled, Yes
Enable Space Limit	Specifies the maximum total space (in MB) that a user's iFolder data is allowed to use, across all iFolders the user owns for the selected user account. Deselect this option if there is no individual user quota or to accept the system-wide quota for the selected user account. Select this option to enforce a user quota; then specify the total space quota (in MB) for the selected user account. If you enable a user space limit that is less than a user's current total space for iFolder data, the user's data stops synchronizing until the data is decreased below the limit or until the quota is increased to a value that is larger than the user's total space consumed. Default Value: Disabled or the system-wide quota if it is set
Enable File Type Restriction	Deselect this option to allow all file types to be synchronized or to apply the system-wide file type restrictions for the user account. Select this option to restrict some file types for this user, and then specify the inclusion or exclusion filters that determine the file types that can be synchronized for the user account.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-14**

Policy	Description
Enable File Type Restriction (*continued*)	To add a file extension to an inclusion or exclusion filter, type the extension (such as .mpg), and then select OK to apply the filter. To edit an extension, select the value, click Edit (the pen icon), modify the entry, and then select OK to apply the change. Default Value: Disabled, Allow all file types; or the System-wide settings
Minimum Synchronization Interval	Deselect the check box to set no synchronization interval or to accept the system-wide setting for the user account. If no value is set for system-wide or user policies, the value reported is No Limit. Select the check box to enable a minimum synchronization interval, and then specify the minimum interval (in seconds). For example, a practical value is 600 seconds (10 minutes). Default Value: Disabled, or the system-wide policy

Manage iFolders

To perform basic iFolders management tasks from iManager, you need to know how to do the following:

- Create an iFolder in iManager
- Create an iFolder from the User Page
- Search for an iFolder
- Configure an iFolder
- Share an iFolder

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Create an iFolder in iManager

To create an iFolder in iManager, do the following:

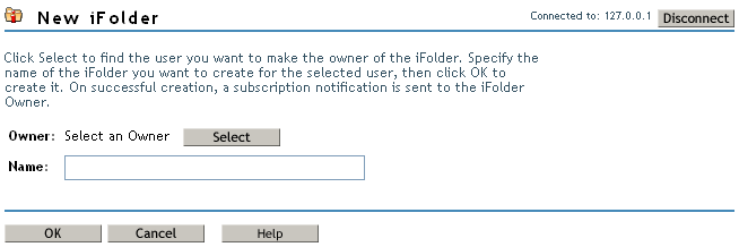
1. Under iManager Roles and Tasks (on the left), expand the **Novell iFolder 3** role; then select **iFolders**.

 A Search page appears.

2. Select the **New iFolder** link.

 The following appears:

Figure 8-23



3. To the right of Owner, select **Select**.
4. Search for the ***user*** that you want to make the owner of the iFolder and select the ***User*** check box; then select **OK**.

 On the New iFolder page, the Owner field shows the user's first and last name.

5. Enter a ***name*** for the iFolder.
6. Create the iFolder by selecting **OK**.

 When the iFolder is successfully created, a subscription notification is sent to the iFolder Owner.

 The new iFolder is listed alone in the Search Results area.

7. Select the iFolder's ***name*** link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Create an iFolder from the User Page

To create an iFolder from the user page in iManager, do the following:

1. Under iManager Roles and Tasks, expand the **Novell iFolder 3** role; then select **Users**.
2. Search for and select the ***name*** of the user you want to manage; then select **OK**.

 A User page opens displaying the user's information.
3. From the User page, select the **iFolders** tab; then select **New**.

 A Create an iFolder dialog box appears.

 The user appears in the Owner field.
4. Enter a ***name*** for the iFolder.
5. Create the iFolder by selecting **OK**.

 When the iFolder is successfully created, a subscription notification is sent to the iFolder Owner.

 The new iFolder is listed alone in the Search Results area.
6. Select the iFolder's ***name*** link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Search for an iFolder

To search for an iFolder in iManager, do the following:

1. From iManager, expand the **Novell iFolder 3** role.
2. Use one of the following methods to get a list of iFolders:
 - Select the **iFolders** role to open the Search iFolders page and specify your ***search criteria***; then select **OK**.

 or

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Select **Orphaned iFolders** on the iFolders page or select the **Orphaned iFolders** role to retrieve a list of orphaned iFolders.

3. Use one of the following search methods; then select **Search**:
 - Select **Equals** as the filter criterion; then type the ***name*** of the iFolder you want to locate in the Search iFolders field.
 - Select a ***filter criterion*** (Contains, Begins With, Ends With, Equals) for the name of the iFolder; then type one or more ***letters*** in the Search iFolders field.
 - Type an asterisk (*) in the Search iFolders field to return a list of all iFolders on the system.
 - Leave the Search iFolders field empty to return a list of all iFolders on the system.

 Do not click anywhere in the page until the page completely refreshes, and then you can browse, sort, or manage the iFolders listed in the Search Results report.
4. Browse or sort the list of iFolders to locate the iFolder you want to manage.
5. Select the iFolder's ***name*** link to view its details, change the owner, configure its policies, share the iFolder, or modify members' access rights.

Configure an iFolder

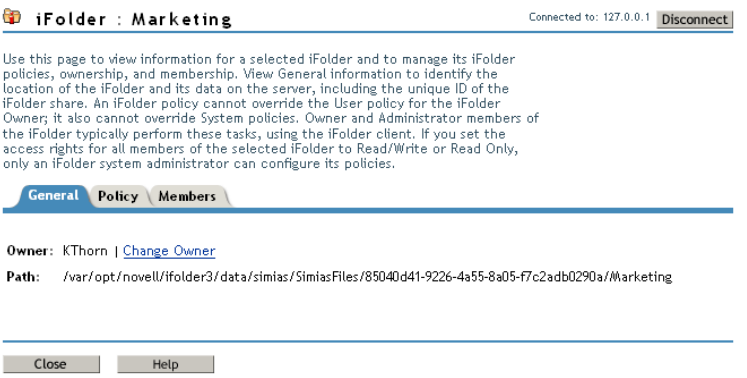
To configure an iFolder from iManager, do the following:

1. From iManager, select the **Novell iFolder 3** role; then select **iFolders** or **Orphaned iFolders**.
2. Locate the iFolder you want to manage; then select the iFolder's ***name*** link.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-24



The following describes the information displayed on the General tab:

Table 8-15

Parameter	Description
Owner	The username of the owner of the selected iFolder. For orphaned iFolders, the iFolder Admin user is made the custodial owner until the iFolder can be reassigned or deleted. The iFolder owner has the Full Control right to the iFolder. The owner manages membership and access rights for users, and can remove the Full Control right for any member. With an enterprise server, the disk space used by the owner's iFolders counts against the owner's user account quotas on the enterprise server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-15**

Parameter	Description
Path	The actual location of the iFolder and its data on the server. For example: /var/opt/novell/ifolder3/simias/SimiasFiles/e84fdc6e-3d51-49df-ae3f-8c9213c76994/iFolder_Name In this example, e84fdc6e-3d51-49df-ae3f-8c9213c76994 is the unique ID of the iFolder share.

3. Select the **Policy** tab; then select the **Modify** link.

 The following appears:

Figure 8-25



4. Enable a policy by selecting a ***check box***; then specify a ***value*** for the policy and apply it by selecting **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following describes each policy:

Table 8-16

Policy	Description
Synchronization Enabled	Select Synchronization Enabled to allow the synchronization of data in the iFolder. Deselect Synchronization Enabled to turn off synchronization, usually temporarily. Default Value: Enabled, Yes
Enable Space Limit	Select the Enable Space Limit check box; then specify the maximum size (in MB) for the selected iFolder. If you enable a system-wide iFolder quota, a user's account quota overrides it, whether the user quota is lower or higher than the system quota. Default Value: Disabled, No Limit
Space Used (View only)	Reports how much space the iFolder data currently consumes.
Enable File Type Restriction	To enable filtering, select Enable File Type Restriction. Specify one of the following methods to filter files that are synchronized: ■ Select "Allow All File Types Except," and then specify the list of file types to exclude when iFolder synchronizes files in the iFolder. ■ Select "Only Allow the Following File Types," and then specify the list of file types to include when iFolder synchronizes files in the iFolder. Type a file extension, and then select OK to add it to the list.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-16**

Policy	Description
Enable File Type Restriction (*continued*)	To edit an extension, select the value, select Edit (the Pen icon), modify the entry, and then select OK to apply the change. Default Value: Disabled, No restriction
Minimum Synchronization Interval	Select the Synchronization Interval check box to enable a minimum interval setting for the selected iFolder, and then specify the minimum value in seconds that users are allowed to set on their clients. To disable the setting, deselect the Synchronization Interval check box. If the option is disabled, the value reported is No Limit. If this option is enabled, the minimum synchronization interval specifies the minimum interval in seconds at which a user's client can check iFolder data on the server and local iFolders to identify files that need to be downloaded or uploaded. The effective minimum synchronization interval is always the largest value from the following settings: ■ The system policy (default of zero (0)), unless a user policy is set. If a user policy is set, the user policy overrides the system policy, regardless of whether it is larger or smaller in value. ■ The local machine policy, or the setting on the client machine synchronizing with the server. ■ The iFolder (collection) policy. Default Value: Enabled, 0 seconds

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Share an iFolder

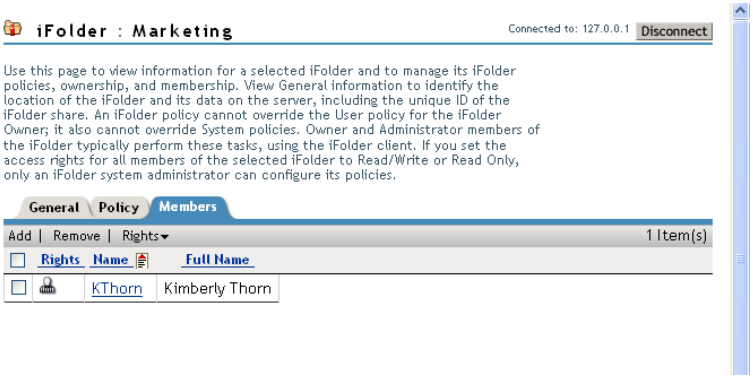
To share an iFolder from iManager, do the following:

1. From iManager, select the **Novell iFolder 3** role; then select **iFolders** or **Orphaned iFolders**.
2. Locate the iFolder you want to manage; then select the iFolder's ***name*** link.

 The iFolder's General tab page appears.
3. Select the **Members** tab.

 A list of members similar to the following appears:

Figure 8-26



4. Select **Add**.
5. Search for the user you want to make a member and select the ***check box*** next to the user's name; then select **OK**.

 The user is given Read Only access to the iFolder by default.
6. (Optional) Select the ***user*** check box; then select the **Rights** drop-down list and specify the Access right as Full Control, Read/Write, or Read Only.

 Wait for the page to refresh.

 The user's icon should reflect the new access right.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

A notification message inviting the user to participate is sent to the user's account.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 5 Manage iFolder 3.*x* as a User

Once you have installed iFolder 3.*x* and provisioned users, users can perform some iFolder management tasks from the iFolder client.

The following are some of the basic tasks users can perform:

- Manage iFolder Accounts and Preferences
- Manage iFolders
- Use Novell iFolder 3.x Web Access



For additional information on managing iFolder 3.*x* as a user, see the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Manage iFolder Accounts and Preferences

To manage iFolder accounts and preferences with the iFolder client, you need to know how to perform the following basic tasks:

- Start the iFolder Client
- Configure an iFolder Account
- Log In to an iFolder Account
- View and Modify iFolder Account Settings
- Configure iFolder Preferences for the Client

Start the iFolder Client

To start iFolder for Novell Linux Desktop 9, do the following:

1. Log in to your computer with the user identity you want to use when you create iFolders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. Use one of the following methods to start iFolder:
 - Open a terminal window; then enter one of the following:

 /opt/novell/ifolder3/bin/ifolder

 or

 ifolder
 - If you want iFolder to start automatically when you log in, make sure iFolder is running when you log out of your GNOME session; then save the session.

 You can also open a terminal window, log in as the root user, and then run **/opt/gnome/bin/gnomesession-properties** to add iFolder as a program to start up when you log in to your computer.
3. (Conditional) If you disabled Remember Password for your iFolder account, you must log in to the account to synchronize the User list, synchronize iFolders, and manage your iFolders.



You do not need to start iFolder on SUSE Linux Enterprise Desktop 10; it automatically starts for you when you log in to the desktop.

To start iFolder for Windows 2000/XP/2003, do the following:

1. Log in to the computer with the Windows user identity you want to use when you create iFolders.
2. (Conditional) If iFolder does not start automatically on successful login, start iFolder by selecting **Start > Programs > iFolder**; then select the **iFolder** application.

 iFolder does not start automatically if you disable the "Start iFolder When Logging In to the Desktop" setting in iFolder Preferences.
3. (Conditional) If you disabled Remember Password for your iFolder account, you must log in to the account to synchronize the User list, synchronize iFolders, and manage your iFolders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Configure an iFolder Account

You must configure at least one iFolder account before you can create iFolders or share iFolders on your system. You can create only one account for any given host computer or server, but you can have multiple accounts.

A user with a different local login and user account can log in to the same computer at a different time and use iFolder to create his or her own set of iFolders under that identity.

iFolder synchronizes only iFolders belonging to the active user.

Configure an iFolder account by doing the following:

1. Use one of these methods to access account setup:
 - The first time you start iFolder after the installation, iFolder prompts you to set up an iFolder account.

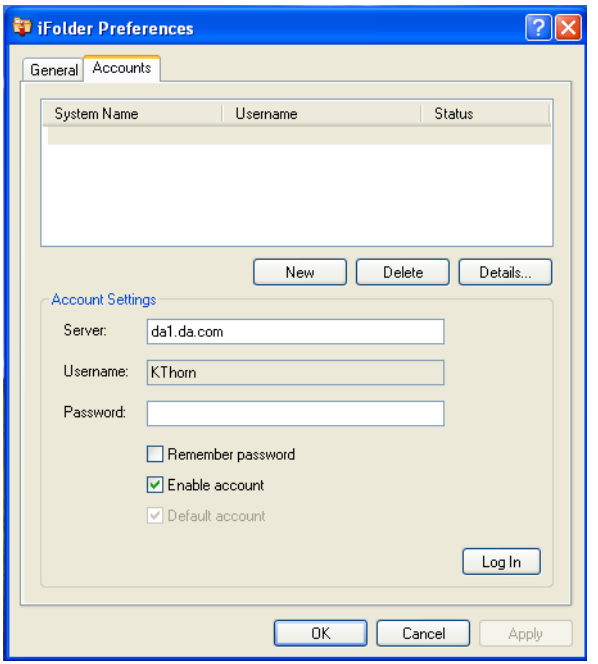
 Select **Yes** to go directly to the iFolder Preferences > Accounts tab.

 or
 - Right-click the **iFolder application** icon in the Notification area; then select **Accounts**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

An iFolder Preferences dialog box appears with the Accounts tab page displayed:

Figure 8-27



2. Access the Account Settings area of the Accounts tab page by selecting **New**.
3. In the Account Settings area, specify the following information:

Table 8-17

Parameter	Description
Server	The DNS name or IP address of the iFolder enterprise server where you have an account. For example: da1.da.com or 10.200.200.1.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-17**

Parameter	Description
Username	Enter your user identity for this account. The iFolder administrator decides whether the format you should use is your network user ID (LDAP common name) or your email address. For example, if your name is John Smith with a user ID of jsmith and an email address of john.smith@example.com, your administrator configures a setting for the server that determines which of the two formats to accept in the Username field for authentication purposes.
Password	The password for your username.
Remember Password	Select Remember Password to log in automatically to this iFolder account whenever you log in to your computer. If your network password changes, automatic authentication fails gracefully the next time iFolder attempts to log in to the iFolder account. iFolder prompts you to log in with your new password and allows you to specify and save the new password.
Enable Account	Select Enable Account to allow background synchronization of iFolder invitations, the user list, and iFolders for this account.
Default Account	Select Default Account to make this account the one selected by default in the drop-down list of accounts when you create iFolders.

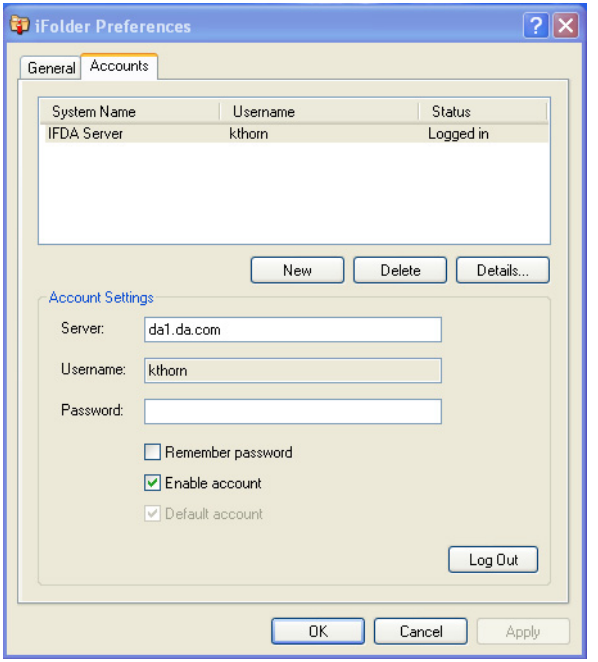
4. When you finish, select **Log In**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

5. (Conditional) If you are prompted with a certificate, review the certificate or certificate message; then select **OK** to accept it.

6. Verify that the account is created by checking that the account appears in the list of accounts with a status of Logged In, as in the following:

Figure 8-28



iFolder begins synchronizing any existing iFolders, iFolder notifications, and the user list for that account.

This initial download can take a few seconds to a few minutes, depending on the size of the user list for the account.

7. Close the iFolder Preferences dialog box by selecting **OK**.

8. Set up iFolders for the account using either of the following methods:

 - If iFolders are available for the account, an iFolder Notification message pops up. Select the message to open the iFolders dialog.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

or

- If there are no iFolders for the account or if you want to start adding iFolders, right-click the **iFolder application** icon; then select **iFolders** to open the iFolders dialog.

Log In to an iFolder Account

After you set up an iFolder account, you must log in whenever you want to synchronize your local iFolder data, the list of iFolder users, and your shared iFolder notifications.

You can be logged in to multiple accounts concurrently. Use one of the following login methods for each account:

- **Enable Remember Password** so that login to the iFolder account occurs automatically whenever you log in to your desktop or start the iFolder client.

 Whenever your password changes, automatic authentication fails gracefully the next time iFolder attempts to log in to the iFolder account.

 iFolder prompts you to log in with your new password and allows you to specify and save the new password.

 or

- **Disable Remember Password** and log in to an iFolder account only when you are ready to synchronize files in its iFolders or to manage the iFolders.

To enable or disable Remember Password for an existing iFolder account:

1. Right-click the **iFolder Services** icon in the Notification area; then select **Accounts**.
2. Select the ***iFolder account*** to view its account settings.
3. Select (enable) or deselect (disable) **Remember Password**.
4. Enter the ***password***; then select **OK** or **Apply**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

5. Select **OK** to verify the change to the Account settings, or select **Cancel** to back out of the change.

To log in to an iFolder account:

1. Right-click the **iFolder Services** icon in the Notification area; then select **Accounts**.
2. Select the ***iFolder account*** to view its account settings.
3. Enter the ***password***; then select **Log In**.

 On successful login, the account's status changes to Logged In.

 If login fails, an error message reports the cause, such as password failure.
4. Close the Accounts dialog box by selecting **OK**.

View and Modify iFolder Account Settings

To view or modify iFolder account settings, do the following:

1. Right-click the **iFolder Services** icon in the Notification area; then select **Accounts** to open iFolder Preferences to the Accounts tab.
2. Select the *account* to view or modify the following parameters:

Table 8-18

Parameter	Description
Server	The DNS name or IP address of the iFolder enterprise server where you have an account. For example: da1.da.com or 10.200.200.1.
Username	Enter your user identity for this account. The iFolder administrator decides whether the format you should use is your network user ID (LDAP common name) or your email address.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-18**

Parameter	Description
Username (*continued*)	For example, if your name is John Smith with a user ID of jsmith and an email address of john.smith@example.com, your administrator configures a setting for the server that determines which of the two formats to accept in the Username field for authentication purposes. You can create only one account per enterprise server.
Password	The password for your username.
Remember Password	Select Remember Password to log in automatically to this iFolder account whenever you log in to your computer. If your network password changes, automatic authentication fails gracefully the next time iFolder attempts to log in to the iFolder account. iFolder prompts you to log in with your new password and allows you to specify and save the new password.
Enable Account	Select Enable Account to allow background synchronization of iFolder invitations, the user list, and iFolders for this account. This governs only client-side functions. The status of whether an account is Enabled or Disabled is shown in the Status column of the Accounts list. You can view status of the Enable Account setting at a glance if you have more than one account set up. When you use iFolder with Novell iFolder 3.*x*, the iFolder system administrator can disable your iFolder account (usually temporarily) on the server side.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-18**

Parameter	Description
Enable Account (*continued*)	You can expect the following behavior: ■ If you are logged in when the account is disabled from the server side, you can manage your iFolders and your iFolder data continues to synchronize with the server until you end your session by logging out or disabling synchronization, or until the server disconnects your session, whichever occurs first. ■ If the account is disabled on the server side, you receive a pop-up message informing you that the account is disabled whenever you attempt to log in. Contact your iFolder system administrator for assistance.
Default Account	Select Default Account to make this account the one selected by default in the drop-down list of accounts when you create iFolders.

3. On the Accounts tab in iFolder Preferences, select the ***iFolder account***; then select **Details** to view the following information about your iFolder Account:

Table 8-19

Parameter	Description
Server	The host name of the enterprise server. For example, if the server's DNS name is da1.da.com, da1 is the information reported.
Description	The user-friendly description of the enterprise server, simple server, or workgroup host computer as entered by its administrator. If no description was entered, the value is None.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-19**

Parameter	Description
Available	The total amount of space currently available to you for iFolders on this iFolder account. The value is equal to the quota minus the used space.
Used	The total amount of space currently consumed by all the iFolders you own on this account.
Quota	The total amount of space allocated to your iFolder account on the enterprise server. This value might be the default quota set for all users, or a user-specific quota. If no quota is set, the value is empty or N/A (Not Applicable).

Configure iFolder Preferences for the Client

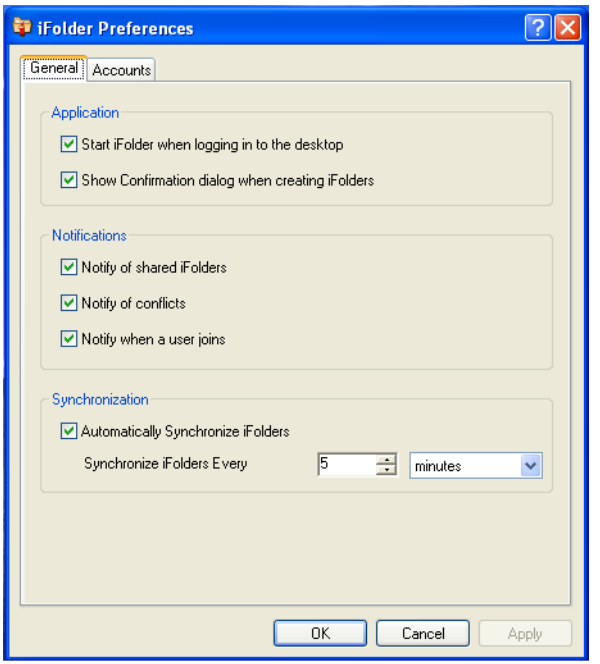
To configure iFolder client preferences, do the following:

1. Right-click the **iFolder Services** application icon in the Notification area; then select **Preferences**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The iFolder Preferences dialog box appears with the General tab page displayed:

Figure 8-29



2. Select or enter the following:

Table 8-20

Parameter	Description
Start iFolder When Logging In to the Desktop	Select this option to launch iFolder whenever you log in with the local username where you set up the iFolder account. For those accounts where you have enabled Remember Password, synchronization occurs in the background at the specified Synchronization Interval. Deselect this option to start iFolder manually.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-20**

Parameter	Description
Show Confirmation Dialog When Creating iFolders	Select this option to receive a confirmation message each time you create an iFolder. This message appears in addition to the normal visual cues such as the iFolder appearing in the list of iFolders. Deselect this option to stop receiving the confirmation message.
Notify of Shared iFolders	Select this option to enable a pop-up message in the Notification area whenever you receive a new invitation to share an iFolder. Invitations are retrieved based on the Synchronization Interval you specify in iFolder Preferences. The interval controls the synchronization of files, iFolder share invitations, and the list of users. You can also click Refresh to update invitations on demand. Deselect this option to disable the pop-up message behavior for invitations.
Notify of Conflicts	Select this option to enable a pop-up message in the Notification area whenever a conflict occurs when synchronizing files. Deselect this option to disable the pop-up message behavior for synchronization conflicts.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-20**

Parameter	Description
Notify When a User Joins	Select this option to enable a pop-up message in the Notification area whenever a user accepts an invitation to share an iFolder. Acceptance is keyed to when the user actually sets up the iFolder on his or her own computer. Deselect this option to disable the pop-up message behavior for user share confirmation.
Synchronization	■ **Automatically Synchronize iFolders.** Select this check box to enable synchronization for all iFolders on this computer under your current local login/logon identity. Deselect the check box to disable synchronization. ■ **Synchronize iFolders Every.** Specify the minimum interval to use for synchronizing iFolders on this computer under your current local login/logon identity. Specify the value and units. If you use the iFolder client with Novell iFolder 3.*x*, the effective minimum synchronization interval is always the largest value of the following settings: ■ The system policy (default of zero (0)), unless a user policy is set.
Synchronization (*continued*)	If a user policy is set, the user policy overrides the system policy, regardless of whether the user policy is larger or smaller in value. ■ The local machine policy or the setting on the client machine synchronizing with the server. ■ The iFolder (collection) policy.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

3. When you finish, save your changes by selecting **Apply**.
4. Close the iFolder Preferences dialog box by selecting **OK**.

Manage iFolders

An iFolder is a local directory used to selectively share and synchronizes files with user-specified members.

The iFolder files are accessible to all members and can be modified and read by those with privileges to do so.

The following are basic tasks for managing iFolders from the iFolder client:

- Create an iFolder
- Share an iFolder
- Set Up an Available iFolder
- View and Configure Properties of an iFolder
- Synchronize Files
- Delete an iFolder



For complete details on managing iFolders, see "Managing iFolders" on page 47 in the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Create an iFolder

You can create an iFolder by converting an existing folder. If the folder does not exist, you can browse to a location and create the new folder as part of the process.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Within the iFolder, you can set up any subdirectory structure that suits your personal or corporate work habits.

The subdirectory structure is constant across all member iFolders. Each workstation can specify a different parent directory for the shared iFolder.

To create iFolders, you need to know how to do the following:

- Create iFolders in a File Manager
- Create iFolders in the iFolders Browser
- Create iFolders on a FAT32 Mount Point (Linux)

Create iFolders in a File Manager

To create an iFolder from a file manager, do the following:

1. Use the file manager to navigate to the folder you want to convert to an iFolder; then select the ***folder***.
2. Do one of the following:
 - Right-click the folder icon ; then select **Convert to an iFolder**.

 or

 - From the toolbar, select **File > Convert to an iFolder**.

 The folder icon changes to a folder with an overlay of the iFolder icon .
3. When the iFolder Created message appears, do one of the following:
 - Close the message by selecting **Close**.

 or

 - Disable future notifications by selecting **Do Not Show This Message Again**; then select **Close**.

 If you later decide that you want to receive confirmation messages, go to iFolder Preferences, select **Show Confirmation Dialog When Creating iFolders**, and then select **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

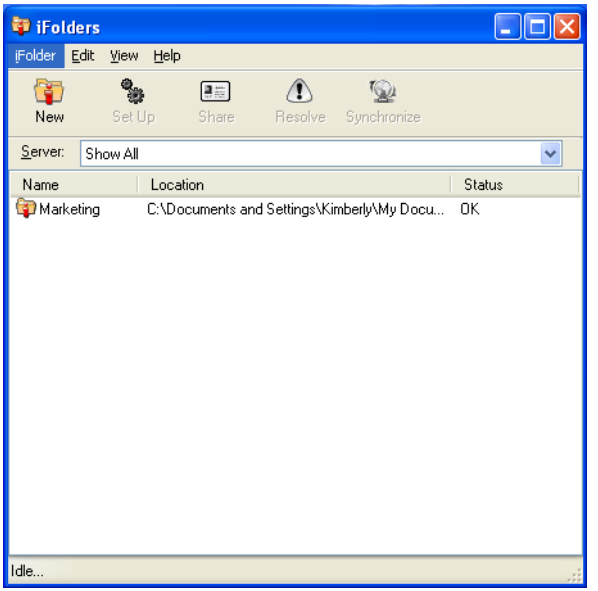
Create iFolders in the iFolders Browser

To create an iFolder in the client iFolders browser, do the following:

1. From the Notification area, right-click the **iFolder** icon ; then open the iFolders browser by selecting **iFolders**.

 The following appears:

Figure 8-30



2. Select **New**.

 A New iFolder dialog appears.

3. (Conditional) If you have multiple iFolder accounts, specify the ***iFolder account*** you want to use for this iFolder.

 The default account is listed first. Use the drop-down list to select a different account.

4. To the right of the Location field, select **Browse**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-31



5. In the browser, navigate to the ***directory*** where you want to create an iFolder.
6. Select the ***normal folder*** you want to make an iFolder by doing one of the following:
 - If the normal folder exists, select the ***folder***; then select **OK**.

 or

 - If the normal folder does not exist, select **Make New Folder** to create it, select the newly created ***folder***; then select **OK**.
7. When you finish, select **OK**.

 The iFolder appears in the iFolders list.
8. When the iFolder Created message appears, do one of the following:
 - Close the message by selecting **Close**.

 or

 - Disable future notifications by selecting **Do Not Show This Message Again**; then select **Close**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If you later decide that you want to receive confirmation messages, go to iFolder Preferences, select **Show Confirmation Dialog When Creating iFolders**, and then select **OK**.

Create iFolders on a FAT32 Mount Point (Linux)

On Linux, iFolder supports creating and using iFolders on a mount point for a FAT32 file system.

Before you can create new iFolders or set up shared iFolders on a FAT32 volume on your Linux computer, the iFolder user must own the FAT32 mount point where you want to store the iFolders, and the /etc/fstab file must explicitly identify the iFolder user's local user ID for the mount point.



This is required because FAT32 does not support file permissions. Any other file system that does not support permissions would have the same issue.

For dual boot systems, you can access the data in iFolders just as you would data in a normal folder.

If you set up the folder as an iFolder on both platforms, the data set is stored in two different iFolders on the server, which consumes twice as much of your allocated server disk resources.

Because the FAT32 file system does not support POSIX file system permissions, make sure the iFolder user is the local owner of the mount point.

Modify the /etc/fstab file to set the user ID (UID) parameter of the user's local login identity to the iFolder user who creates iFolders on that mount point by doing the following:

1. Log in to your computer as the **root** user.
2. From a command prompt, create the directory where you want to mount the FAT32 file system by entering the following:

 mkdir /home/*username*/*fsmount*

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Replace ***username*** with the username of the user who plans to use the FAT32 drive for iFolders. Replace ***fsmount*** with the directory name you want to use as the mount point.

For example, if the username is jsmith and the directory name is fat32mntpt for a FAT32 drive or partition, you would enter the following:

mkdir /home/jsmith/fat32mntpt

3. Mount the FAT32 drive at the desired mount point by entering the following:

 mount -t vfat */dev/hda1* /home/*username*/*fsmount*

 Replace ***/dev/hda1*** with the device or partition name of the non-Linux device. Replace ***username*** with the username of the iFolder user. Replace ***fsmount*** with the directory name you want to use as the mount point.

 For example, if the FAT32 file system (vfat) is on the hda4 device (/dev/hda4), the username is jsmith, and the mount point directory is /home/jsmith/fat32mntpt, you would enter

 mount -t vfat /dev/hda4 /home/jsmith/fat32mntpt

4. Edit the /etc/fstab file by adding the uid=*username* parameter of the iFolder user on the line that defines the FAT32 mount point, such as the following:

 ***/dev/hda1* /home/*username*/*fsmount* vfat uid=username**

 In the jsmith example, you would modify /etc/fstab file by adding uid=jsmith to the mount point, as in the following:

 /dev/hda4 /home/jsmith/fat32mntpt vfat uid=jsmith

Share an iFolder

To share an iFolder, you need to know how to do the following:

- Add a User to an iFolder
- Modify User Access Rights
- Remove a User from an iFolder

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Add a User to an iFolder

You can add a user to an iFolder by doing one of the following:

- **Add a user with a file manager.** To add a user with a file manager, do the following:

 1. From the file manager, navigate to and select the ***iFolder***.
 2. Right-click the ***iFolder***: then select **iFolder > Share with**.
 3. From the list of users, select one or more ***users***.
 4. Select the access right: **Full Control**, **Read/Write**, or **Read Only**.
 5. Select **Apply**.

- **Add a user with the iFolders browser.** To add a user with the iFolders browser, do the following:

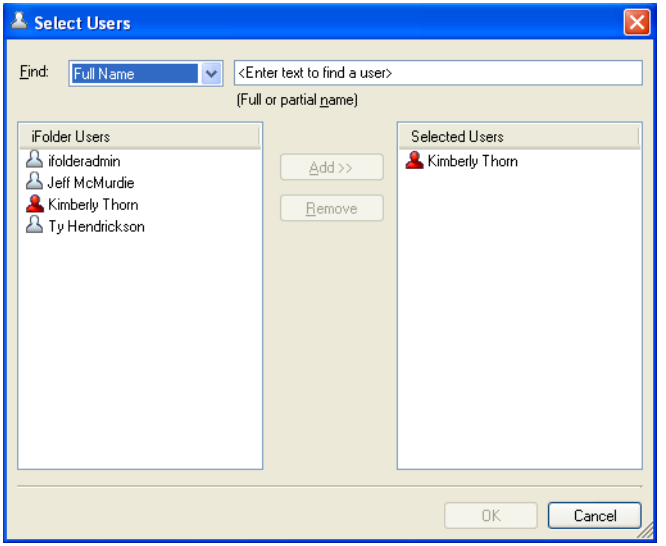
 1. In the Notification area, right-click the **iFolder** icon  , then select **iFolders** to open the iFolders browser.
 2. From the list of iFolders, select the ***iFolder***; then select **Share**.

 The iFolder Properties dialog opens with the Sharing tab selected.
 3. Select **Add**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following appears:

Figure 8-32



4. From the list of users, select one or more ***users***; then add them to the Selected Users list by selecting **Add**.
5. When you finish, select **OK**.

 It can take several seconds for the invitations to synchronize to the server.
6. Select one or more ***users***; then select **Access**.
7. Select the **Full Control**, **Read/Write**, or **Read Only** access right.
8. When you finish, select **OK**.
9. Select **Apply**; then close the iFolder Properties dialog by selecting **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Modify User Access Rights

As the working relationships and status of members of an iFolder change, you might need to change a user's access right setting for the iFolder.

For example, you might want to give a trusted user the File Control right for the iFolder.

To set user rights for an iFolder, you can do one of the following:

- **Set user rights with a file manager.** To set user rights with a file manager, do the following:

 1. From the file manager, navigate to the iFolder; then select it.
 2. Right-click the ***iFolder***; then click **iFolder > Share with**.
 3. From the list of users, select one or more ***users***.
 4. Select **Access**; then select the **Full Control**, **Read/Write**, or **Read Only** right.
 5. Select **Apply**; then close the iFolder Properties dialog by selecting **OK**.

- **Set user rights with the iFolders browser.** To set user rights with the iFolders browser, do the following:

 1. From the Notification area, right-click the **iFolder** icon  ; then open the iFolders browser by selecting **iFolders**.
 2. From the list of iFolders, select the ***iFolder***; then select **Share**.
 3. From the list of users, select one or more ***users***.
 4. Select **Access**; then select the **Full Control**, **Read/Write**, or **Read Only** right.
 5. Select **Apply**; then close the iFolder Properties dialog by selecting **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Remove a User from an iFolder

To unshare an iFolder, you must remove a user as a member of the iFolder. The iFolder on the user's workstation becomes a normal folder.

A copy of the data remains on the former member's workstation, but the files are no longer synchronized with the shared iFolder.

You can remove a user from an iFolder by doing one of the following:

- **Remove users with a file manager.** To remove a user with a file manager, do the following:

 1. From the file manager, navigate to the ***iFolder***; then select it.
 2. Right-click the ***iFolder***; then select **iFolder > Share with**.
 3. From the list of users, select one or more ***users***.
 4. Select **Remove**; then select **Apply**.
 5. Select **OK**.

- **Remove users with the iFolders browser.** To remove a user with the iFolders browser, do the following:

 1. In the Notification area, right-click the **iFolder** icon  ; then open the iFolders browser by selecting **iFolders**.
 2. From the list of iFolders, select the ***iFolder***; then select **Share**.
 3. From the list of users, select one or more ***users***.
 4. Select **Remove**; then select **Apply**.
 5. Select **OK**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Set Up an Available iFolder

When others share iFolders with you, the iFolders appear with an Available iFolder icon in your iFolders browser.

To participate in the shared iFolder on your current local computer, you need to set up the iFolder to make it active on the computer.

To set up an iFolder, do the following:

1. In the Notification area, right-click the **iFolder** icon ; then open the iFolders browser by selecting **iFolders**.
2. From the list of iFolders, select the available ***iFolder***; then select **Set Up**.
3. (Conditional) If you are not logged in to the account, log in with your ***username*** and ***password***; then select **OK**.
4. Browse to and select the ***location*** where you want to create a local iFolder.
5. Select **OK** twice.

View and Configure Properties of an iFolder

You can use the iFolders Properties page to view and configure the information about a selected iFolder.

To access the iFolders Properties page, you can do one of the following:

- **Access iFolder properties from a file manager.** To access the Properties dialog from a file manager, right-click the ***iFolder***; then select **iFolder > Properties**.
- **Access iFolder properties from the iFolders browser.** To access the Properties dialog from the iFolders browser, right-click the iFolder icon in the Notification area; then select **iFolders** to open the iFolders browser.

 From the list of iFolders, select the ***iFolder***, then select **Properties**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

On the Properties page, the following parameters report the disk space used on the iFolder server:

Table 8-21

Parameter	Description
Available	The total amount of server disk space currently available for files or directories in the selected iFolder. The value is equal to the quota minus the used space.
Used	The total amount of server disk space currently consumed by all files and directories in the selected iFolder.
Set Quota *or* Quota	■ **Set Quota.** If you are the iFolder owner, you can specify a quota for the iFolder. ■ **Quota.** If you are a member, the value reports the total amount of server disk space allocated to the selected iFolder by the iFolder owner. If no quota is set, the value is empty or N/A (Not Applicable).

The following parameters report the synchronization status for the local copy of the iFolder:

Table 8-22

Parameter	Description
Last Successful Synchronization	The completion time of the most recent successful synchronization of your local copy of the iFolder with the iFolder server.
Files/Folders to Synchronize	The total number of storage items (files and folders) in the iFolder that need to be synchronized.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 8-22**

Parameter	Description
Automatically Synchronizes Every	The synchronization interval for the iFolder. Specify the value in minutes, hours, or days. When the iFolder client is used with a Novell iFolder 3.*x* enterprise server, the interval cannot override the minimum interval specified by the iFolder administrator for the server or your account on the server, but it can override the client-wide synchronization interval.
Synchronize Now	Select the button to initiate a synchronization on demand.

Synchronize Files

To synchronize iFolder files, you need to know how to do the following:

- **Synchronize files on demand.** To synchronize files on demand, do the following:

 1. In the Notification area, right-click the **iFolder** icon  ; then open the iFolders browser by selecting **iFolders**.
 2. From the list of iFolders, select the ***iFolder***.
 3. Do one of the following:
 - Select **Synchronize**.

 or

 - Select **iFolder > Synchronize now**.

- **Configure the synchronization interval.** To configure the synchronization interval, do the following:

 1. In the Notification area, right-click the **iFolder** icon  ; then open the iFolder Preferences dialog box by selecting **Preferences**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. From the General tab page, do one of the following:
 - Enable background synchronization by selecting **Automatically Synchronize iFolders**.

 or

 - Disable background synchronization by deselecting **Automatically Synchronize iFolders**.
3. (Conditional) If you enable synchronization, specify the ***interval*** for synchronizing files (such as every 1 hour or every 2 days).

 When the iFolder client is used with Novell iFolder 3.*x*, the minimum system Synchronization Interval, typically every 5 minutes, is configured by the iFolder administrator.

 You cannot override the system minimum. The absolute system minimum is 1 minute.

Delete an iFolder

If you delete an iFolder from your collection, it deletes the local copy of the iFolder and its contents. It also can affect the share relationship for the iFolder, depending on the Access right you hold for it.

Deleting an iFolder does not uninstall the iFolder client from your workstation.

To delete an iFolder, do the following:

1. From a file manager or iFolders browser, locate the ***iFolder*** that you want to delete.
2. Right-click the ***iFolder***; then select **Delete**.

The following outlines the effect on the share relationship and the member iFolders based on the Access right of the user who deletes the iFolder:

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Table 8-23

Access Right of the User Who Deletes the iFolder	Effects
Owner	Ends the share relationship for the iFolder: ■ **Server copy of the iFolder:** Deletes the iFolder metadata and contents from the server. ■ **Member copies of the iFolder:** Reverts the iFolder to a normal folder for all users.
Full Control User	Unsubscribes the user from the share: ■ **Server copy of the iFolder:** No effect. ■ **Member copies of the iFolder:** Reverts the local copy of the iFolder to a normal folder.
Read/Write User	Unsubscribes the user from the share: ■ **Server copy of the iFolder:** No effect. ■ **Member copies of the iFolder:** Reverts the local copy of the iFolder to a normal folder.
Read Only User	Unsubscribes the user from the share: ■ **Server copy of the iFolder:** No effect. ■ **Member copies of the iFolder:** Reverts the local copy of the iFolder to a normal folder.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Use Novell iFolder 3.x Web Access

Novell iFolder 3.*x* Web Access provides an interface that gives users remote access through a web browser to iFolders on the enterprise server.

To use Novell iFolder 3.x Web Access from a supported web browser, you need to know how to do the following:

- Log In and Log Out
- Browse iFolders
- Manage Folders and Files in an iFolder



For complete details on using Web Access, see "Using Novell iFolder 3.x Web Access" on page 59 in the *Novell iFolder User Guide for Novell iFolder 3.x* (user.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Log In and Log Out

You can log in to Novell iFolder 3.*x* Web Access to gain access to folders and files in any of the iFolders available to you in your Novell iFolder enterprise server account.

This includes iFolders that you participate in but have not set up on a local computer. (You cannot access 2.1*x* iFolders with Web Access.)

The enterprise server specified in the URL authenticates your username against the server's LDAP directory services.

You can also specify which of the supported localized interfaces to use. This is typically the Language Code of the iFolder enterprise server. Make sure to configure your browser's Languages setting to support the desired language.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

To log in to Web Access, do the following:

1. From a supported Web browser, enter the ***URL*** of the iFolder server where your iFolders are stored:

 http://*servername.example.com*

 Replace ***servername.example.com*** with the DNS name or IP address (such as da1.da.com or 10.200.200.1).

2. From the left navigator panel of the OES Welcome page, open the iFolder 3.*x* Welcome page by selecting **iFolder 3.x**.

3. In the iFolder Links on the right, open the login dialog by selecting the **Web Access** link.

4. From the iFolder 3.x Web Access Login dialog, enter your account ***username*** and ***password***.

5. From the Languages drop-down list, select the ***language*** you want to use to access your files.

6. Select **OK**.

 This login gives you access only to those iFolders in the same domain as the server you specified in the URL.

 To log in to a different server, enter its server's URL in your web browser, and then log in.

7. When you finish with Web Access, log out by selecting **Logout** (upper right header area); then close your browser.

 If you do not log out, your session remains open until your session times out, which can be a security risk.

 If the system connection times out when you are working in your iFolders, Web Access returns you to the Login dialog. You can log in again to resume working without closing your browser.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Browse iFolders

The iFolders page lists all iFolders available to you in the current domain. Available iFolders include those you own and those others have made available to you.

You can access iFolders through Web Access even if you have not set up the iFolder on a local computer. The Owner column identifies the name of the person who owns the iFolder to help you locate the iFolder you seek.

Select the iFolder's name to view a list of its folders and files, upload and download files, create folders, and delete folders and files.

Manage Folders and Files in an iFolder

Within an iFolder, you can do the following:

- **View a list of folders and files.** The iFolder page lists folders and files alphabetically. Scroll to locate the directory or file of interest.
- **Navigate directories.** Select the name of the folder  to open the folder and view a list of its contents. To return to a higher-level directory, select the Up Folder icon  in the task bar.
- **Download a file.** Select the name of the file you want to download; then select one of the following:
 - **Open.** View the file's contents by selecting Open.

 You must have a compatible application on your computer to open the file.

 The file is downloaded to a temporary folder, such as Temporary Internet Files in Windows, where Internet files are saved and then opened with your local application.

 If you plan to work in the file, it is best to save the file locally, modify the file, and then upload it.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Save.** Save the file locally or to a mapped drive by selecting **Save**.

 Navigate to the location where you want to place the file, and then select **Save**. The file is downloaded to your computer.

Options on the page might differ slightly, depending on the web browser you use.



iFolder 3.*x* Web Access does not support the uploading and downloading of 10 MB or larger files.

- **Create a new folder.** In the New Folder field, specify the name of the new folder, and then select **Create**.

 Folder names are case sensitive. When the page refreshes, the folder appears alphabetically in the list.

- **Delete folders or files.** Select the check box next to one or more folders or files you want to delete; then select **Delete** and confirm the deletion.

- **Upload a file.** In the Upload File field, select Browse, locate a local folder you want to upload, and then select **Open > Upload**.

 When the page refreshes, the file appears alphabetically in the list.

 The maximum file size for the upload limit is configured by the administrator. By default, the limit is set to 10 MB; the limit for your server might differ.



iFolder 3.*x* Web Access does not support the uploading and downloading of 10 MB or larger files.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise 8-2 Use iFolder 3.x on the Windows XP Professional and SLED 10 Workstations

Now that you have installed and configured iFolder 3 on the DA1 Linux server, and have provisioned users for access to iFolder, you are ready to test using iFolder 3.x on a Windows XP Professional and a SLED 10 workstation.

You do this by performing the following tasks:

- Install the iFolder client on the Windows XP Professional workstation.
- Set up and use an iFolder account on the Windows XP Professional workstation.
- Set up and use the iFolder client on the SLED 10 workstation.

Exercise 8-2 Use iFolder 3.x on the Windows XP Professional and SLED 10 Workstations is in your *Integrating Novell Open Enterprise Server for Linux Workbook* on page 8-16.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Summary

Objective	Summary
1. Describe the Purpose and Architecture of iFolder 3.x	To describe the purpose and architecture of iFolder 3.*x*, you learned about the following: ■ **Benefits of iFolder for the enterprise.** Benefits of iFolder to the enterprise include the following: ■ Seamless data access ■ Data safeguards and data recovery ■ Reliable data security ■ Productive mobile users ■ Cross-platform client support ■ Scalable deployment ■ Simple data and account management ■ No training requirements ■ **Benefits of iFolder for users.** Novell iFolder provides the following benefits for users: ■ Guards against local data loss by automatically backing up local files to the iFolder server and multiple workstations ■ Transparently updates a user's iFolder files to the iFolder enterprise server and multiple member workstations with the iFolder client

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
1. Describe the Purpose and Architecture of iFolder 3.x (*continued*)	■ Tracks and logs changes made to iFolder files while users work offline, and synchronizes those changes when they go online ■ Provides access to user files on the iFolder server from any workstation without the iFolder client, using a web browser and an active Internet or network connection ■ With SSL encryption enabled, protects data as it travels across the wire ■ Makes files on the iFolder server available for regularly scheduled data backup ■ **Enterprise server sharing.** The iFolder client included in this release supports synchronization across multiple computers through a central Novell iFolder 3.*x* enterprise server. ■ **How iFolder 3.*x* works.** Novell iFolder 3.x supports multiple iFolders per user, user-controlled sharing, and a centralized network server for file storage and secure distribution. ■ Key components of iFolder. The following are the key components of iFolder 3.*x*: ■ iFolder enterprise server ■ Novell iFolder 3 plug-in to Novell iManager 2.5 ■ iFolder Web access ■ The iFolder client

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
1. Describe the Purpose and Architecture of iFolder 3.x (*continued*)	■ Shared iFolders ■ iFolder access rights ■ Account setup for enterprise servers ■ Access authentication ■ File synchronization and data management ■ Synchronization log ■ iFolder client APIs
2. Plan for an iFolder Services Installation	In this objective, you were introduced to planning considerations for providing Novell iFolder 3.*x* services on OES Linux, which include the following: ■ Security considerations ■ Server workload considerations ■ Naming conventions for usernames and passwords ■ Admin user considerations ■ iFolder user account considerations ■ iFolders data and synchronization considerations ■ Management tools
3. Install Novell iFolder 3.x and iFolder Web Access	To install Novell iFolder 3.x and iFolder Web Access, you learned about the following: ■ Prerequisites and installation guidelines ■ How to install iFolder on an existing OES Linux server ■ How to configure the iFolder Enterprise server

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
3. Install Novell iFolder 3.x and iFolder Web Access (*continued*)	■ How to configure the iFolder Web Access server ■ How to install the Novell iFolder 3 plug-in for iManager ■ How to access iManager and the Novell iFolder 3 plug-in ■ How to provision users and iFolder services
4. Manage iFolder 3.x as an Administrator	Once you have installed iFolder 3.x and provisioned users, you are ready to begin managing iFolder. In this objective you learned about the following basic tasks for managing iFolder 3.*x* on an OES Linux server as an Administrator: ■ Distribute and install the iFolder client ■ Start, stop, and restart the iFolder services ■ Manage the Simias log and Simias access log ■ Recover individual files or directories ■ Configure system policies ■ Modify the iFolder LDAP settings ■ Manage the iFolder Web Access server ■ Configure iFolder users ■ Manage iFolders

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
5. Manage iFolder 3.x as a User	Once you have installed iFolder 3.*x* and provisioned users, users can perform some iFolder management tasks from the iFolder client. The following are some of the basic tasks you learned about that users can perform: ■ Manage iFolder accounts and preferences ■ Manage iFolders ■ Use Novell iFolder 3.*x* Web Access

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

SECTION 9 Configure White Pages (eGuide)

In this section, you learn how to configure eGuide on an OES Linux server.

Objectives

1. Describe the Purpose and Architecture of eGuide
2. Perform Basic eGuide Administration Tasks

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Introduction

Novell eGuide lets you use the information in eDirectory to create a "white pages" directory for your organization that users can access from their web browser.

eGuide offers many options. To provide these options, you configure the components that eGuide needs, such as LDAP, search categories, languages, and the eGuide display.

In this section, you learn how to access and use eGuide and perform some basic eGuide configuration tasks on an OES Linux server.



For complete information about configuring Novell eGuide, see the *Novell eGuide 2.1.2 Administration Guide* (eguide.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 1 Describe the Purpose and Architecture of eGuide

To describe the purpose and architecture of eGuide, you need to know the following:

- What eGuide Provides
- eGuide System Requirements
- How eGuide Works
- How to Access the eGuide Client

What eGuide Provides

eGuide is a browser-based solution that lets your employees search for people and places regardless of your LDAP data source location.

eGuide looks like an address book. But unlike an ordinary address book, eGuide is platform- and application-independent. It can be accessed through a standard web browser by any user with rights to your web server.

You can use eGuide to search Novell eDirectory as well as multiple LDAP data sources at the same time.

For example, if your company purchases another company, you can provide a combined white pages view of both companies using eGuide pointing at two separate directories.

eGuide runs on the most widely used platforms and is compatible with email, instant messaging, and real-time collaboration tools, such as AOL Instant Messenger or Microsoft NetMeeting.

When users find the people they are looking for, eGuide lets them launch the type of communication that fits their current needs—email, instant messaging, and even video conferencing.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following is a list of eGuide features:

- Standards-based display and administration using HTML, XML, and XSL, which provides simple, convenient, and customizable configuration
- Advanced searching on any attribute
- Data handler controls that let you display information the way you prefer
- Organizational charts that are automatically generated based on eDirectory attributes
- Anonymous and User Authentication modes, including contextless login, cookies, and support for eDirectory password restrictions
- Authenticated searching that uses access control lists in eDirectory to determine if a user can access particular attribute information, such as home phone numbers
- Seamless integration with Novell iChain and Novell exteNd Director
- Compatibility with eDirectory or any other LDAP-enabled directory service

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

eGuide System Requirements

The following are the minimum system requirements for setting up and using eGuide 2.1.2:

Table 9-1

System Component	Minimum Requirement
Operating System	One of the following: ■ NetWare 6 with Support Pack 3 or later ■ Red Hat Linux 7.3 ■ Solaris 8 ■ Windows 2000/XP (recommended) or Windows NT ■ AIX 5L
Web Server	One of the following: ■ Internet Information Server (IIS) 4.0 or later on Windows platforms ■ Apache HTTP server 1.3.26 or later For help installing Apache, visit the Apache Documentation (http://httpd.apache.org/docs-2.0/) web site.
Web Application Server	One of the following: ■ Tomcat servlet container version 3.3a, 3.3.1, or 3.3.1a **NOTE:** Tomcat does not perform optimally on Windows NT. For help installing Tomcat, visit the Apache Jakarta web site (http://jakarta.apache.org/tomcat/tomcat-4.1-doc/index.html). ■ Sun Java 2 Standard Edition (J2SE) 1.3.1 or later ■ IBM Java 1.3.1 for AIX

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 9-1**

System Component	Minimum Requirement
Java Virtual Machine (JVM)	Version 1.4.1 or later
LDAP Directory	■ Supports LDAP v3 ■ Supports Novell eDirectory If you plan to use eGuide with Novell eDirectory (formerly called NDS) as your LDAP directory, Novell eDirectory version 8 or later is the minimum requirement; version 8.5 or later is required to support password security; version 8.6.2 or later is required to support Role-Based Services (version 8.7.1 recommended). ■ Uses clear text passwords for clear text connections; clear text passwords are disabled by default in eDirectory 8.7.1
Browser for eGuide Administration Utility	■ Netscape* 7 or later ■ Internet Explorer 5.5 SP2 or later
Browser for eGuide Client	■ Netscape 4.78 or later (version 7 recommended) ■ Internet Explorer 5.0 or later (version 6 recommended)

How eGuide Works

You can configure eGuide to publish any information that you store in eDirectory.

For example, the default eGuide installation in OES lets users search for the names of all eDirectory user objects on your system. It lets users see the details for their own user objects that are stored in eDirectory, but it doesn't let them modify the eDirectory information.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

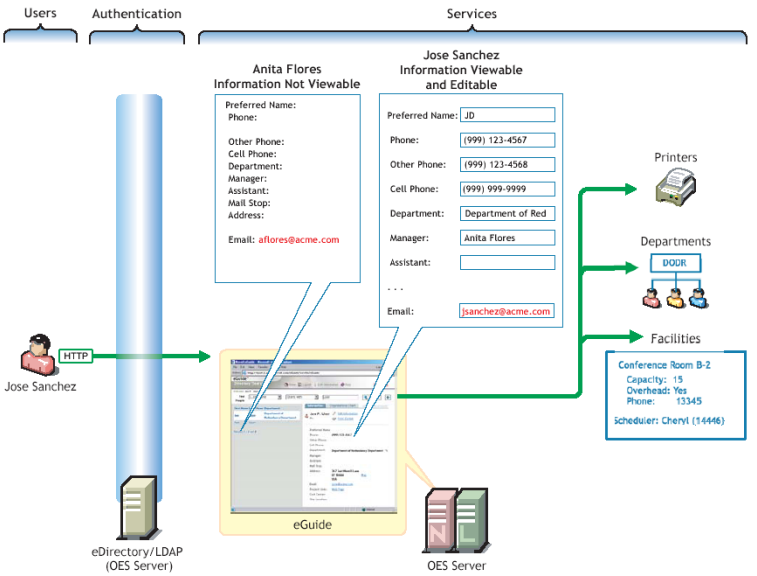
If they access other user objects, they can see only the e-mail address attributes associated with those objects.

You can configure eGuide so that users can see information stored in eDirectory (such as telephone numbers, office locations, and job titles) for other eDirectory users in your organization.

You can also configure eGuide so that users can maintain their own information in eDirectory. You can even let them choose the information they want other users to be able to access.

The following summarizes the eGuide functionality available by default in Novell OES:

Figure 9-1



The following describes Figure 9-1:

- **Users.** An eDirectory user named Jose Sanchez logs in to eGuide.
- **Authentication.** Access to eGuide is controlled through LDAP-based authentication through the eDirectory LDAP server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Although shown separately, eDirectory can be installed on the OES server.

- **Services.** Jose searches using the asterisk (*) wildcard and sees two entries: Anita Flores and Jose Sanchez.

 If he clicks Anita's name, he sees only her email address (by default), but he can see his own information.

 You can configure eGuide so that Jose can edit some of his information and the changes will be stored in eDirectory.

 You can also let users search on any object types in eDirectory, letting them find the people, places, things, and information they need to be productive and self-sufficient.

How to Access the eGuide Client

To access the eGuide client from a supported web browser, do the following:

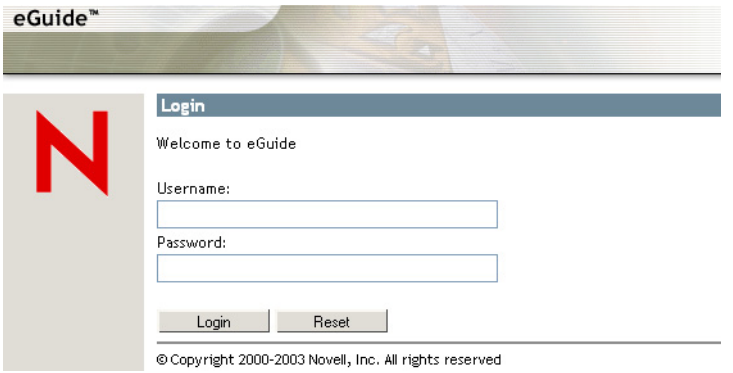
1. Enter the following URL:

 http://*web_server*/eGuide

 Replace ***web_server*** with the hostname or IP address of the web server where you installed eGuide. The eGuide portion of the URL shown above is case sensitive.

 An eGuide login page appears:

Figure 9-2

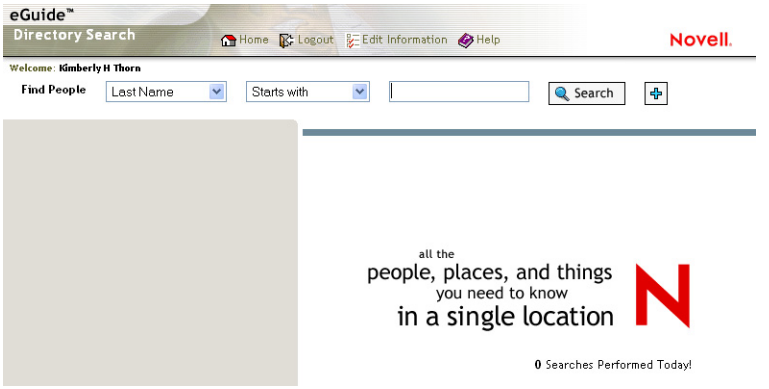


Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

2. Log in with an eDirectory ***username*** and ***password***.

 An eGuide home page appears:

Figure 9-3



You can also access the eGuide client from the eGuide Administration Utility by selecting the **Launch Novell eGuide Client** icon at the top of the web page.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective 2 Perform Basic eGuide Administration Tasks

In this objective, you are introduced to the following basic eGuide administrative tasks:

- How to Access the eGuide Administration Utility
- How to Modify Search Categories
- How to Configure the eGuide Display
- How to Configure Security Restrictions
- How to Enable Display of Organizational Charts for eDirectory Users



For complete information about configuring Novell eGuide, see the *Novell eGuide 2.1.2 Administration Guide* (eguide.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

How to Access the eGuide Administration Utility

To access the eGuide Administration utility, do one of the following from a compatible web browser:

- Access the following case-sensitive URL and log in as the Admin user:

 http://*web_server*/eGuide/admin/index.html

 where ***web_server*** is the host name or IP address of the web server where you installed eGuide. The port number might also be required.

- Log in to the eGuide client as the admin user; then, at the top of the eGuide page, select the **Administrative Utility** icon.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

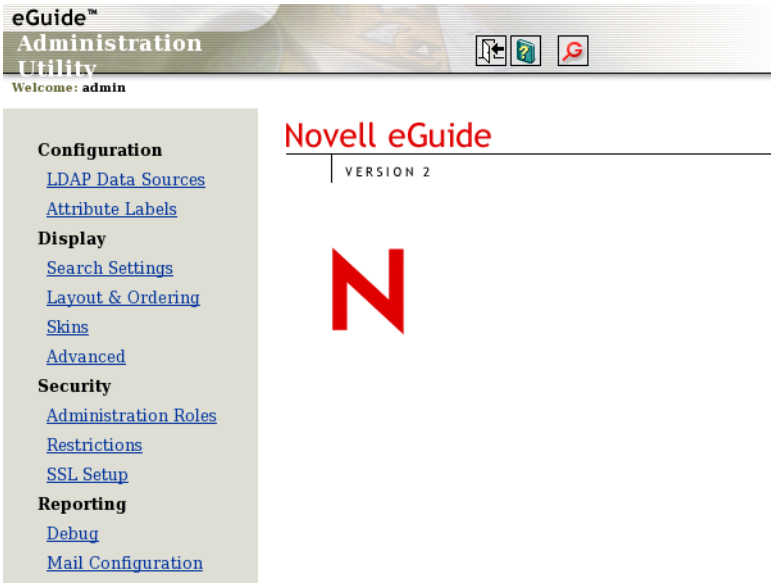
The eGuide Administration utility icon is available only to authenticated users designated as eGuide administrators.

For details, see “Administration Roles” on page 32 in the *Novell eGuide 2.1.2 Administration Guide for Linux* (eguide.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*

After you open the eGuide Administration utility, the following appears:

Figure 9-4



Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How to Modify Search Categories

A *search category* is an entity that eGuide uses to represent a combination of LDAP classes.

For example, when you add the first directory to eGuide, the User search category is created. By default, it includes the following classes: InetOrgPerson, OrganizationalPerson, and Person.

The attributes within these user classes appear in the Attributes page where you configure how eGuide uses them in the eGuide client. Also, the user category label Find People appears in the first search filter drop-down list in the eGuide client.



The InetOrgPerson, OrganizationalPerson, and Person classes are used only if they existed in the first directory you added.

To manage search categories, you need to know how to do the following:

- Add a Search Category
- Remove a Search Category
- Add or Remove Schema Classes from a Search Category

Add a Search Category

To add a search category, do the following:

1. From the eGuide Administration utility, select **LDAP Data Sources**; then select the **Edit** link (for the desired directory).
2. Select **Advanced**; then select **New**.
3. Enter the ***name*** of the new category.
4. Add at least one schema class and configure its associated attributes.
5. When you finish, select **Save**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Remove a Search Category

To remove a search category, do the following:

1. From the eGuide Administration utility, select **LDAP Data Sources**; then select the **Edit** link (for the desired directory).
2. Select **Advanced**.
3. Select the category you want to remove.



User is a mandatory category; eGuide will not let you remove it.

4. Select **Remove *category_name***.

Add or Remove Schema Classes from a Search Category

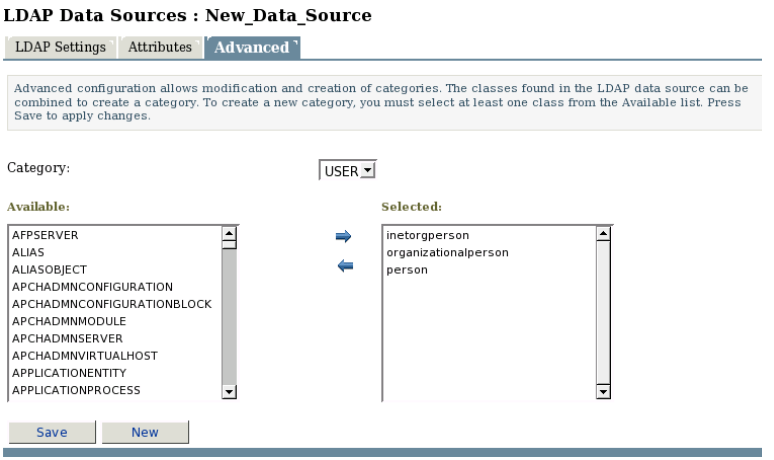
To add or remove schema classes from a search category, do the following:

1. From the eGuide Administration utility, select **LDAP Data Sources**; then select the **Edit** link (for the desired directory).
2. Select **Advanced**.
3. Select the category you want to modify.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A page similar to the following appears:

Figure 9-5



4. Do one of the following:
 - To add a schema class to the category, select the ***class*** from the Available list; then select the **right-arrow** to move the class to the Selected list.

 or

 - To remove a schema class from the category, select the ***class*** from the Selected list; then select the **left-arrow** to move the class to the Available list.
5. When you finish making changes to the category, select **Save**.
6. Do one of the following:
 - If you only removed one or more schema classes, you are done.

 or

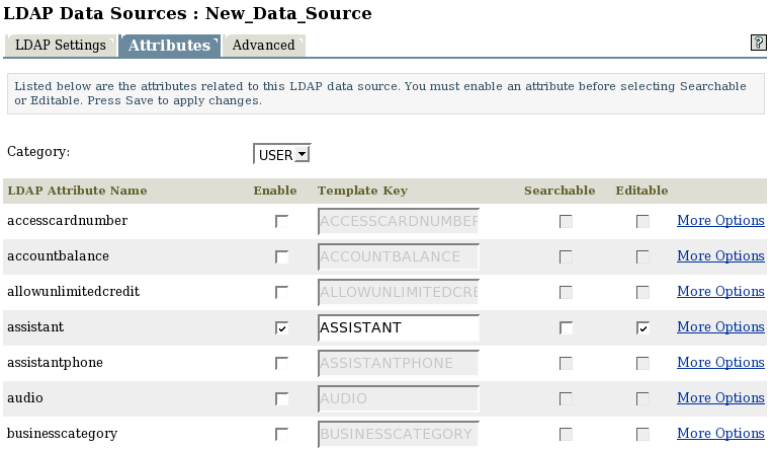
 - If you added one or more classes, continue with Step 8.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

7. Select the **Attributes** tab.

 A page similar to the following appears:

Figure 9-6



8. Edit the settings and mappings for the attributes of the newly added classes; then scroll to the bottom and select **Save**.

 If you added one or more schema classes to a newly added search category, you must enable at least one attribute and make at least one attribute searchable before users can access that category from the eGuide client.

9. Select **Display > Layout & Ordering** to indicate which attributes should be displayed in the Search, List, Details, and Org Chart forms in the eGuide client.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

How to Configure the eGuide Display

The eGuide pages display the features that you make available to users.

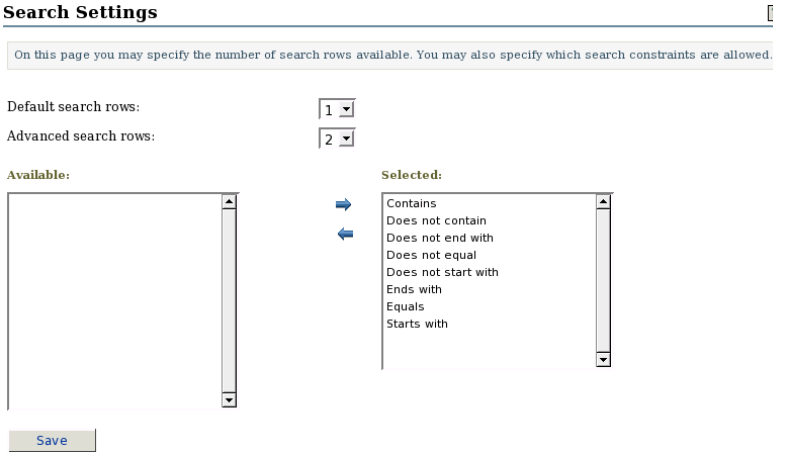
To configure the eGuide pages, you need to know how to do the following:

- Configure Search Settings
- Configure Layout and Ordering
- Change Skins
- Configure Advanced Settings

Configure Search Settings

After logging in as the eGuide administrator, select **Display > Search Settings** to display the following page:

Figure 9-7



The Search Settings let you specify the number of search rows that appear for a normal search and an advanced search (when the user selects the plus sign) in the eGuide client.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

You can also modify the list of search constraints users can select from in each search row.

A search row consists of three drop-down lists:

- One for the search category (such as Users)
- One for the search attribute (such as Last Name)
- One for the search constraint (such as “Starts with...”)

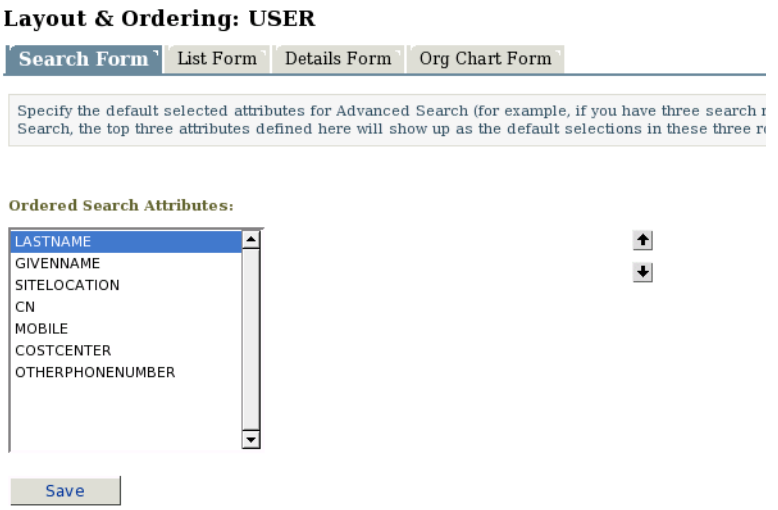
To add a search constraint, select it from the Available list, and then select the right arrow. To remove a search constraint, select it from the Selected list, and then select the left arrow.

Configure Layout and Ordering

The Configure Layout and Ordering page presents a list of all search attributes from all configured directories.

When you select **Edit**, the following tabs appear:

Figure 9-8



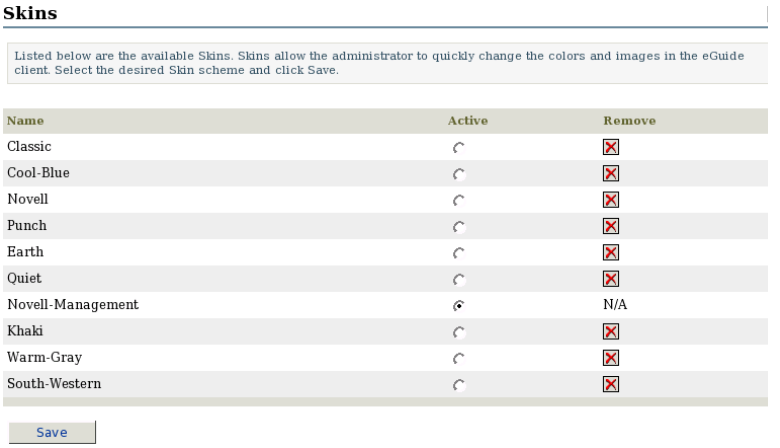
You can select Search Form, List Form, Details Form, or Org Chart Form to view and edit a directory's display settings.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Change Skins

When you select **Skins**, the following appears:

Figure 9-9



eGuide comes with a standard set of skins to use. You can also set up customized skins for your organization.

For details on adding customized skins, see “Adding a Skin or Theme” on page 43 of the *Novell eGuide 2.1.2 Administration Guide* (eguide.pdf).

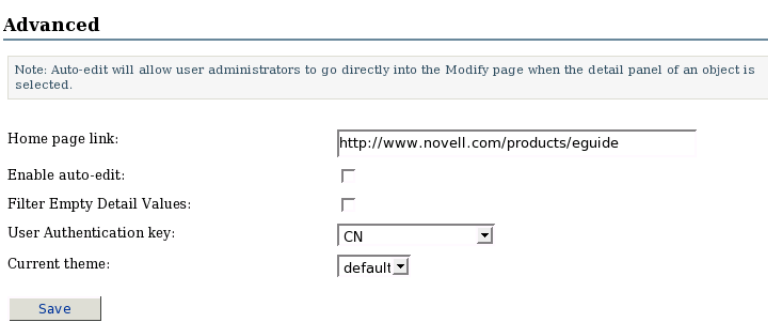
You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Configure Advanced Settings

When you select **Advanced**, the following appears:

Figure 9-10



You can use this page to make additional changes to your eGuide display settings. Select the Help icon (?) for information about each setting. When you finish, select **Save**.

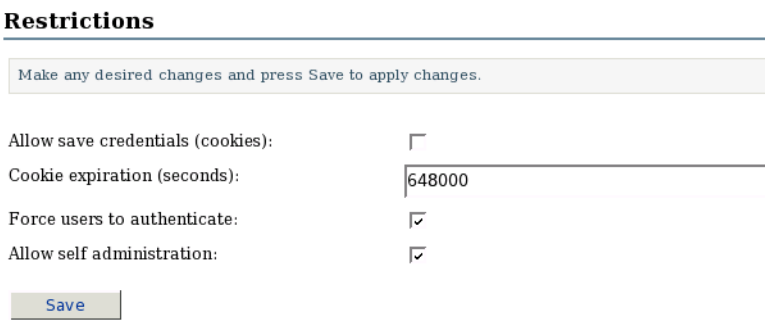
How to Configure Security Restrictions

eGuide security features let you specify who has rights to change the eGuide configuration and LDAP data source attributes.

You can also enforce or remove various security restrictions by selecting **Security > Restrictions**.

The following appears:

Figure 9-11



Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following describes each setting on the Restrictions page:

Table 9-2

Restrictions Setting	Description
Allow Save Credentials	Select this setting if you want users to see a Remember Login Information checkbox on the Login page. If a user selects this option, the user's validated credentials are encrypted and stored in a cookie on the workstation. The user can then load eGuide multiple times without logging in each time. The cookie is removed when the user selects the Logout icon or after the cookie expiration time passes.
Cookie Expiration	Specify the number of seconds you want to elapse between login attempts before the login information cookie expires (86,400 seconds = one day).
Force Users to Authenticate	Select this setting if you want all users to be forced to log in to use eGuide. If this setting is not selected, eGuide loads in anonymous mode. A user then has the option of logging in by selecting the eGuide Login icon. If Allow Save Credentials is on and a login information cookie is available, the user is not forced to reauthenticate.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 9-2**

Restrictions Setting	Description
Show Password Change Link	Select this setting to make the Change Password link available in the Edit panel in the eGuide client. This also allows administrators to change user passwords. "Allow Self Administration" must be selected before users can access the Edit panel.
Allow Self Administration	Select this setting if you want to let users change their editable attributes (those designated as Editable in the Attributes page). When you select Allow Self Administration, the View Personal Information icon in the eGuide client changes to Edit Personal Information.
Show Organizational Chart	Select this setting if you want the Organizational Chart tab activated in the Details panel for all users. The organization chart shows the currently selected user's manager and all of that manager's direct reports.

How to Enable Display of Organizational Charts for eDirectory Users

Organizational (org) chart structure in eGuide is controlled by the Manager and isManager attributes assigned to each user.

The distinguished name in a user's Manager attribute indicates who that user reports to.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A True value in a user's isManager attribute indicates that the user is a manager and activates the Reports To link (left-arrow icon) for traversing upward in the org chart from manager to manager.

By default, only a user's full name (created by combining the FirstName, MI, and SN attributes) and title (if available) is displayed in the org chart.

In addition to the full name, you can display up to four additional attributes (only Title is selected by default) by doing the following:

1. From the eGuide Administration utility, select **Display > Layout & Ordering**.
2. To the right of a displayed category, select **Edit**; then select the **Org Chart Form** tab.
3. From the four attribute drop-down lists, select the ***attributes*** you want displayed (along with the user's full name).

 Only attributes designated as enabled in the Attributes page can be selected.
4. When you finish, select **Save**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise 9-1 Configure and Use eGuide on the DA1 Linux Server

eGuide is automatically installed for you as part of the default Novell OES installation.

In this exercise, you use and configure eGuide for Digital Airlines employees by performing the following tasks:

- View information in eGuide.
- Edit personal information in eGuide.
- Configure attributes as editable by eGuide users.
- Configure the eGuide interface.

Exercise 9-1 Configure and Use eGuide on the DA1 Linux Server is in your *Integrating Novell Open Enterprise Server for Linux Workbook* on page 9-2.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Summary

Objective	Summary
1. Describe the Purpose and Architecture of eGuide	To describe the purpose and architecture of eGuide, you learned about the following: ■ **What eGuide provides.** eGuide is a browser-based solution that lets your employees search for people and places regardless of your LDAP data source location. You can use eGuide to search Novell eDirectory as well as multiple LDAP data sources at the same time. ■ **eGuide system requirements.** In this section, you learned about the minimum system requirements for setting up and using eGuide 2.1.2. ■ **How eGuide works.** You can configure eGuide to publish any information that you store in eDirectory. You can configure eGuide so that users can see information for other users in your organization, such as their telephone numbers, office locations, job titles, and any other information you store in eDirectory. You can also configure eGuide so that users can maintain their own information in eDirectory. You can even let them choose the information they want other users to be able to access.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
1. Describe the Purpose and Architecture of eGuide (*continued*)	■ How to access the eGuide client. To access the eGuide client from a supported web browser, enter the following URL: **http://*web_server*/eGuide** Replace ***web_server*** with the hostname or IP address of the web server where you installed eGuide.
2. Perform Basic eGuide Administration Tasks	In this objective, you were introduced to the following basic eGuide administrative tasks: ■ How to access the eGuide administration utility ■ How to modify search categories ■ How to configure the eGuide display ■ How to configure security restrictions ■ How to enable display of organizational charts for eDirectory users

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

SECTION 10 Provide File Access with NetStorage

In this section, you learn how to provide access to files on Novell OES Linux and OES NetWare servers using NetStorage.

Objectives

1. Describe the Purpose and Architecture of NetStorage
2. Implement and Manage NetStorage

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Introduction

NetStorage makes network files available anywhere, any time, from an Internet web browser.

While iFolder provides personal file storage, synchronization, and access to a specific Simias data collection on the iFolder server, NetStorage provides secure, web-based access to directories and files on OES servers across the network.



For complete details on configuring and implementing NetStorage, see the *Novell OES NetStorage Administration Guide for Linux* (netstor_lx.pdf) and the *Novell OES NetStorage Administration Guide for NetWare* (netstor.pdf).

You can access these guides from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 1 Describe the Purpose and Architecture of NetStorage

To describe the purpose and architecture of NetStorage, you need to know the following:

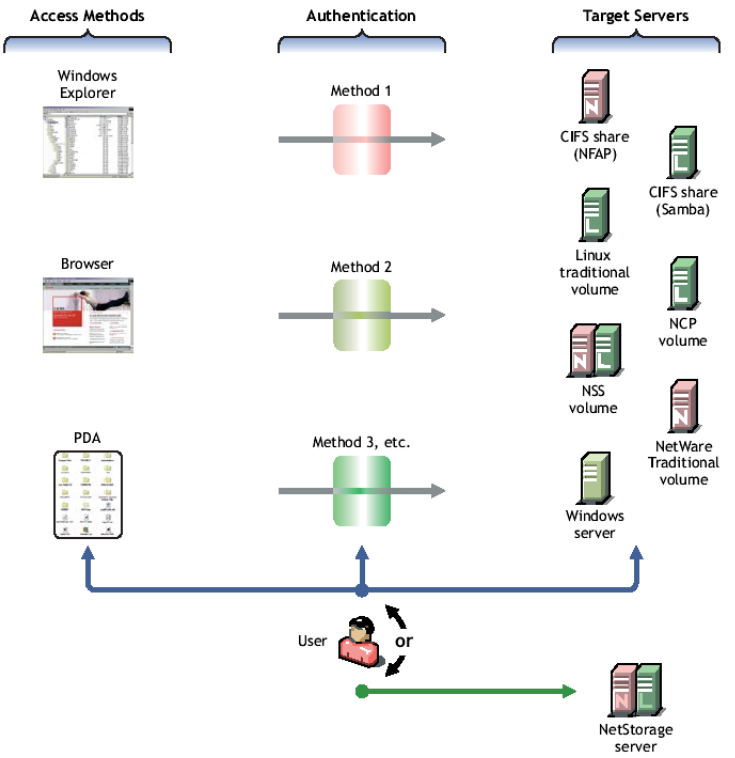
- What NetStorage Provides
- NetStorage System Requirements
- Novell NetStorage on OES Linux
- Novell NetStorage on OES NetWare
- How NetStorage Works
- What Users See When They Access NetStorage

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

What NetStorage Provides

Network file access is often confusing and frustrating to users as illustrated in the following:

Figure 10-1



The following describes Figure 10-1:

- **Access Methods.** Browser or PDA access is business-critical to those who must travel. However, access method support varies widely among file service providers.
- **Authentication.** Authentication helps protect information assets, but having diverse authentication methods leads to frustration and lost productivity.
- **Target File Systems.** Having diverse file storage services only adds to the complexity and confusion.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell NetStorage ties all of these issues together with an easy-to-administer, easy-to-use solution.

NetStorage provides secure Internet-based access to files and folders on Linux and NetWare servers on your network using either a browser or Microsoft Web Folders (Microsoft's implementation of WebDAV).

NetStorage authentication relies on Novell eDirectory to provide secure access, so Internet-based access is as secure as accessing files from within the network.

Novell NetStorage includes the following benefits:

- Lets users securely copy, move, rename, delete, read, and write files between any Internet-enabled machine and Linux or NetWare servers on your network.
- Eliminates the need to use a virtual private network (VPN) client to access files.
- Eliminates the need to email or copy data from one machine to another.
- Supports Internet standards such as HTTP, HTTPS, HTML, XML, and WebDAV.
- Supports the use of drive mappings that users are accustomed to when they log in using the Novell Client.
- Supports access to users' Novell iFolder 2.*x* accounts.
- Provides access to network files and folders via Novell Virtual Office, Novell iFolder 2.*x*, and Novell exteNd Director 4.1 Standard Edition.
- Supports Storage Location objects used to display a specified name for a network directory in the NetStorage directory access list, displayed through Microsoft Web Folders or a web browser.

With NetStorage installed on one OES Linux server, users can potentially have access to any Linux or NetWare 5 or later server anywhere on your geographically dispersed network.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

NetStorage System Requirements

In addition to meeting the requirements for Novell OES, NetStorage requires the following:

- **Server requirements.** At least one Linux server with OES or one NetWare 6.5 server in the Novell eDirectory tree where NetStorage will be installed.

 An eDirectory replica is not required to be on the same server where NetStorage is installed.



To avoid time issues, this server must have time set correctly according to your network specifications. If time is not set, workstations might not be able to access files.

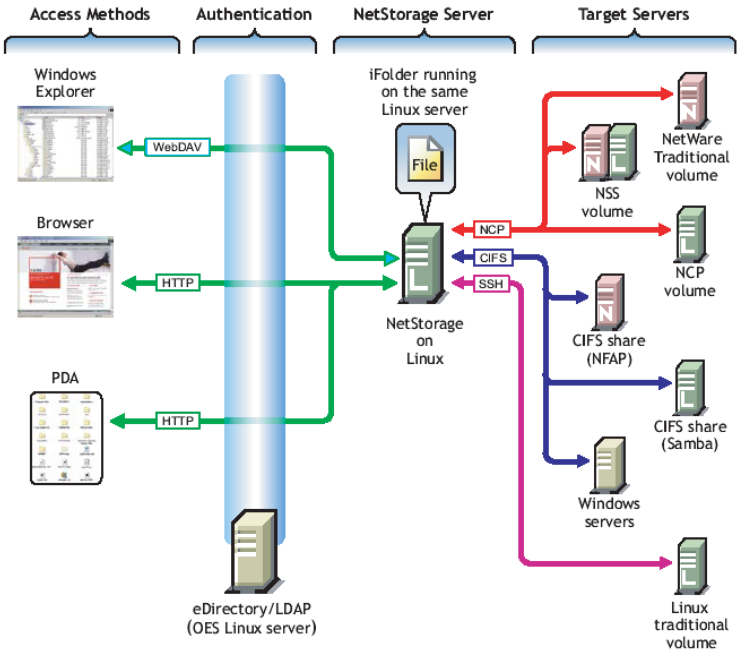
- **Workstation requirements.** Netscape Navigator 4.7 or later, Internet Explorer 5.5 or later, Mozilla, Mozilla Firefox, other Linux browsers, or Microsoft Web Folders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell NetStorage on OES Linux

NetStorage on Linux provides local and Web access to files on many systems without requiring the Novell client, as illustrated in the following:

Figure 10-2



The following describes Figure 10-2:

- **Access methods.** Users have read and write access to files from
 - **Windows Explorer.** This is enabled by the HTTP protocol with WebDAV extensions.
 - **Browsers.** Users can access files directly by connecting to the NetStorage server.
 - **PDAs.** PDA users with network connections can access their files as well.

 Access is granted through login script drive mapping (NCP server required) or through Storage Location objects.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Authentication.** File service access is controlled by LDAP-based authentication through the eDirectory LDAP server.

 Although shown separately, eDirectory could be running on the OES Linux server.

- **NetStorage server.** The NetStorage server receives and processes connection requests and provides access to storage on various servers on the network.

 A Novell iFolder 2.*x* server running on the same server as NetStorage is automatically available through NetStorage to iFolder 2.*x* users.

- **Target servers.** NetStorage on Linux can connect eDirectory users to their files and folders stored in the following locations:

 - The same targets as NetWare (see Figure 10-3) if the NCP server is running
 - Windows workgroup shares (CIFS or Samba shares)
 - Linux traditional volumes through an SSH connection

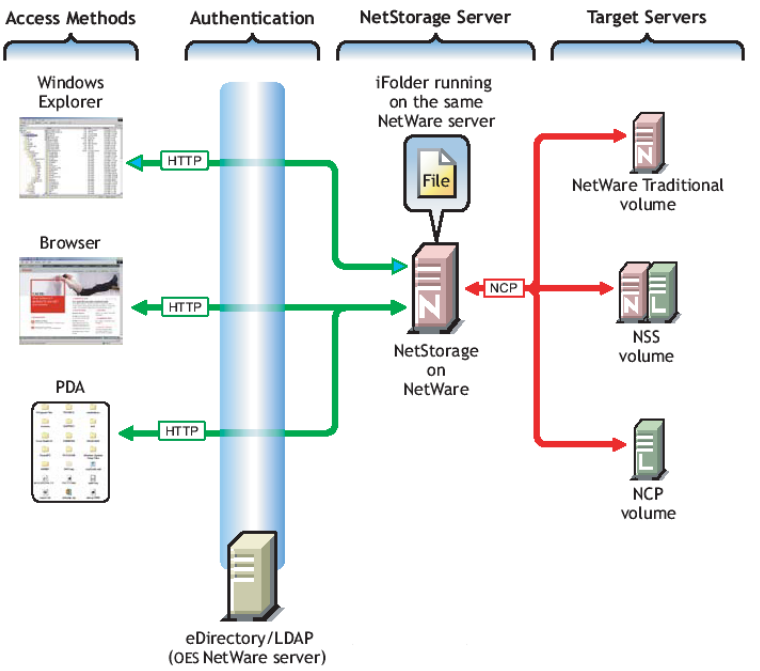
 Linux volumes can also be made available as NCP volumes.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Novell NetStorage on OES NetWare

NetStorage on NetWare provides local and Web access to files on NetWare and Linux without requiring the Novell client, as illustrated in the following:

Figure 10-3



The following describes Figure 10-3:

- **Access methods.** Users have read and write access to files from
 - **Windows Explorer.** This is enabled by the HTTP protocol with WebDAV extensions.
 - **Browsers.** Users can access files directly by connecting to the NetStorage server.
 - **PDAs.** PDA users with network connections can access their files as well.

 Access is granted through login script drive mapping or through Storage Location objects.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Authentication.** File service access is controlled by LDAP-based authentication through the eDirectory LDAP server.

 Although shown separately, eDirectory could be running on the OES NetWare server.

- **NetStorage server.** The NetStorage server receives and processes connection requests and provides access to storage on various servers on the network.

 An iFolder 2.*x* server running on the same server as NetStorage is automatically available through NetStorage to iFolder 2.*x* users.

 You must configure NetStorage if you want access to the iFolder 2.*x* data stored on other servers.

- **Target servers.** NetStorage on NetWare can connect eDirectory users to their files and folders stored in the following locations:

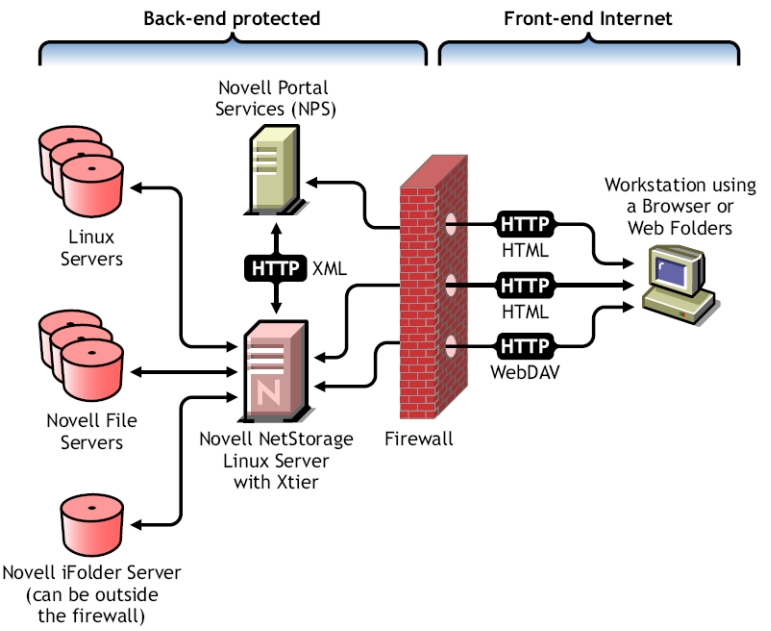
 - NetWare traditional volumes where users have access rights.
 - NSS volumes on either NetWare or OES Linux servers where users have access rights.
 - Any administrator-defined NCP volumes created on an OES Linux server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How NetStorage Works

NetStorage is installed on one Linux server (or NetWare server) that acts as a Middle Tier (also known as XTier) server:

Figure 10-4



Xtier is Novell's Web services framework and is used by various Novell products.

Middle Tier server configuration information is stored in an XML file on the Linux server. Novell iManager provides an easy method for changing Middle Tier configuration.

Previous versions of NetStorage were administered using the NSAdmin utility. Configuration should now be done through Novell iManager.

After the Middle Tier server is set up, it appears as an Internet web server to users and can be accessed either with a web browser or with Microsoft Web Folders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

NetStorage also includes a gadget that provides access through Novell exteNd Director 4.1 Standard Edition.

All transactions can also be encrypted using SSL to increase the security. Novell iFolder 2.*x* transactions are secured using the iFolder encryption mechanism.



It is not currently possible to access iFolder 3.*x* using NetStorage. Because this course does not cover iFolder 2.*x* (only iFolder 3.*x* on Linux), you do not see any iFolder accounts when logging in to NetStorage during the NetStorage exercise.

For details on configuring and implementing iFolder 2.*x* folders to display in a user's NetStorage home page, see the note on page 10 of the *Novell OES NetStorage Administration Guide for Linux* (netstor_lx.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

What Users See When They Access NetStorage

The NetStorage web page displays the network files and folders currently accessible for the logged-in user. The following summarizes NetStorage access:

Table 10-1

OES Platform	Automatic Access
Linux	■ Novell iFolder 2.*x* folders on the same server ■ NSS volumes on the same server that use the default mount point (/media/nss) ■ Drive mapping locations in login scripts of the user logging in (if the NCP Server for Linux is running on the server)
NetWare	■ User Home directories ■ iFolder 2.*x* folders on the same server ■ Drive mapping locations in login scripts of the user logging in

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

To provide access to file systems not listed, you must create Storage Location objects in eDirectory.

For NetWare servers, NetStorage reads the following, and then displays a list of files and folders based on the collected information:

- The user's login script to determine drive mappings
- The eDirectory user object properties to determine the path to the user's home directory
- The user's Novell iFolder 2.*x* account

If Storage Location objects have been created and the user has rights to view these objects, the directories associated with these objects are also displayed.

For example, a default Storage Location object is created when you install NetStorage for the primary authentication domain (such as slc.da).

However, only users in the container (not any subcontainers) are associated with the Storage Location object. You need to create other Storage Location objects (or modify the default object) for users in other containers (or subcontainers) to view directories in the NetStorage web page.

NetStorage reads container, profile, and user login scripts only from the primary eDirectory server specified during the installation. For r NetWare servers, NetStorage displays the user's drive mappings based only on those login scripts.

However, because login scripts were designed to be processed by the Novell client on the user’s workstation, NetStorage processes only a subset of the login script functions.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.



If you specified alternate IP addresses or DNS names of servers in other eDirectory trees during the NetStorage installation, NetStorage reads the user object properties in the other eDirectory trees and also displays those home directories.

This is useful if a user normally logs in to more than one eDirectory tree and you want that user to have access to additional home directories in different eDirectory trees using NetStorage. The User object name must be the same for each eDirectory tree.

NetStorage processes login scripts to find MAP statements. Each MAP statement defines a NetWare file system storage resource that the user will be able to access using NetStorage.

IF, ELSE, END, INCLUDE, and EXIT commands are also recognized by NetStorage. All other login script statements are treated as comments and ignored.

Login script variables are also recognized. Variables are preceded by a percent sign (%).

Because mapped drives do not exist in Linux, you must create and use Storage Location objects to access storage on Linux servers.

If you want to provide users with NetStorage access to a specific folder, you might have to add a drive mapping command to that folder in a login script (container, profile, or user) or create a Storage Location object.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 2 Implement and Manage NetStorage

To perform basic implementation and maintenance tasks on NetStorage, you need to know the following:

- How to Access the NetStorage Home Page
- How to Administer NetStorage from Novell iManager
- How to Create Storage Location Objects and Lists
- How to View or Modify Directory and File Attributes and Rights
- How to Set Directory Quotas on NSS Volumes and Directories
- How to Purge and Salvage Deleted NSS Files
- NetStorage Implementation Guidelines



If your NetStorage installation has an iFolder link, you must complete all the instructions in "Novell iFolder 2.1*x* Implementation and Maintenance" on page 222 in the *Novell OES SP2 Planning and Implementation Guide* (implgde.pdf) before attempting to let users access the service.

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

How to Access the NetStorage Home Page

To access and log in to the NetStorage home page from a browser window on a workstation, do the following:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox); then enter the URL for NetStorage:

 https://*server_ip_address*/oneNet/NetStorage

 Replace ***server_ip_address*** with the IP address or DNS name of the server running NetStorage, or the IP address for Apache-based services.

 If Apache-based services use a port other than 80, you must also specify that port number with the URL.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

For example, if the IP address for NetStorage is 10.200.200.1 and the port number is 51080, then you would enter **https://10.200.200.1:51080/oneNet/NetStorage**.



If you have the Persistent Cookies feature enabled, the date and time on the workstation being used to access NetStorage should be within 24 hours of the date and time on the server running NetStorage in order to avoid conflicts.

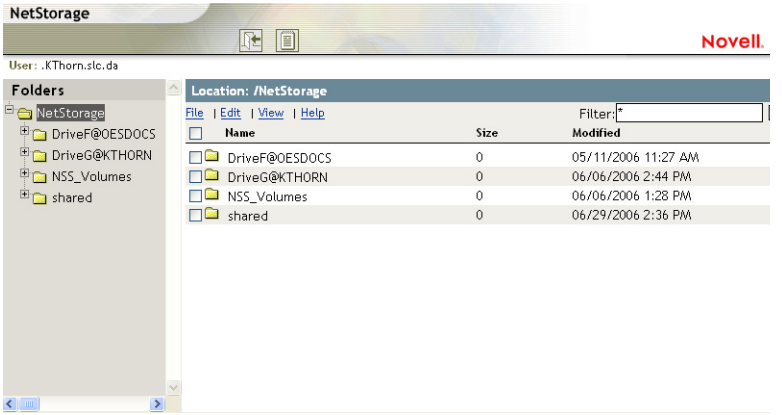
A login dialog appears.

2. Enter an eDirectory ***username*** and ***password***.

 NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

 A NetStorage home page similar to the following appears:

Figure 10-5



You can use many of the same conventions for expanding and contracting folders and opening files that are available in Windows Explorer.

To create new folders or copy, paste, delete, rename, move, upload, or download existing files using a browser, select the **File** menu.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If you are using Internet Explorer, you can copy and move files and folders by dragging and dropping them. This functionality is not available with browsers other than Internet Explorer.

Selecting the **Folder View** button in the browser window displays folders in another column and lets you expand and contract folders.

The Text View displays only the files and folders in the current directory and does not let you expand or contract folders. Selecting the Name, Size, or Modified headings lets you sort directory and file listings in ascending or descending order by name, size, or date.

You can use NetStorage to access local files and folders in a shared directory on the Linux server where NetStorage is installed.

This is useful for uploading files to the local Linux server. The path to the shared folder is /var/opt/novell/netstorage/shared.

You cannot map drives or change login scripts from NetStorage.

3. When you finish, from the top of the page, select the **Logout** icon; then close the web browser window.

How to Administer NetStorage from Novell iManager

You can change your NetStorage configuration after NetStorage has been installed on a Linux or NetWare server (known as the Middle Tier or XTier server) by using Novell iManager.

NetStorage configuration information is stored in an XML file on the Linux server. iManager provides an easy method for changing the NetStorage configuration in the XML file.

After changing any settings, you must restart the Apache Web server. To do this on a Linux server, from a command prompt enter **rchttpd stop**. Wait for a minute; then enter **rchttpd start** to restart the web server. You must also restart xTier by entering **rcnovell-xsrvd restart**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



The following only describes the NetStorage administrative tasks available from iManager.

For complete details on each task and available options, see the online Help available from iManager or "Administering NetStorage" on page 23 of the *Novell OES Netstorage Administration Guide for Linux* (netstor_lx.pdf)

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

To administer NetStorage from iManager, do the following:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox; then enter the following URL for iManager:

 https://*server_ip_address*/nps/iManager

 where ***server_ip_address*** is the IP address or DNS name of the server running iManager.

2. Log in as **admin** (or equivalent user) with the appropriate ***password***.

3. In the left column, expand the **File Access (NetStorage)** role; then select the ***task*** you want to use to configure NetStorage.

 The following describes each task:

 - **Authentication Domains.** Lets you change or add the Novell eDirectory server URLs and contexts that are required by NetStorage.

 This page also lets you add support for dotted usernames, email address names, and Universal passwords, as well as giving you the option to change the eDirectory server that is designated as the Primary.

 - **Current Sessions.** Displays a report with information on the current NetStorage sessions.

 - **Files.** Displays the NetStorage Web page. This provides a way to access NetStorage from iManager, without entering the NetStorage URL.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **iFolder Storage Provider.** View or edit iFolder-specific configuration settings (if you have Novell iFolder 2.*x* installed on your Linux server).
- **NetWare Storage Provider.** Lists configuration options specific to NetStorage on a NetWare server.
- **NetStorage Options.** Lets you configure NetStorage options such as Session Timeout and Persistent Cookies.
- **NetStorage Statistics.** Displays a report with information about server up time, login failures, and number of NetStorage sessions.
- **Resource Usage.** Displays a detailed report of resource utilization for NetStorage.
- **WebDAV Provider.** Lets you edit the moniker used by users to access the NetStorage home page.
- **Storage Location.** Lets you create a Storage Location object to display a specified name for a network directory in the NetStorage directory access list displayed through Microsoft Web Folders or a web browser.
- **Assign Storage Location To Object.** Lets you associate one or more Storage Location objects with a User, Group, Profile, or Container object. Users will see the directory associated with the object the next time they log in.
- **Edit Storage Location.** Modify an existing Storage Location object to change its display name, directory location, or comment.
- **Delete Storage Location.** Delete an existing Storage Location object.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How to Create Storage Location Objects and Lists

After installing NetStorage, you might be able to see only your iFolder 2.*x* directory and a local shared directory on the Linux server using NetStorage.

Storage Location objects are required for accessing files and directories on Linux servers unless you have the NCP server component of OES installed. They can also be used on NetWare servers.

Without an NCP server, users might have specific eDirectory rights to certain files and folders on your network but they will not be able to access those files and folders using NetStorage unless storage location objects have been created.

To create Storage Location objects and lists, you need to know the following:

- How to Create a Storage Location Object
- How to Create a Storage Location List
- How to Create SSH Storage Location Objects

How to Create a Storage Location Object

To create a Storage Location object, do the following:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox; then enter the URL for iManager:

 https://*server_ip_address*/nps/iManager

 Replace ***server_ip_address*** with the IP address or DNS name of the server running NetStorage, or the IP address for Apache-based services.

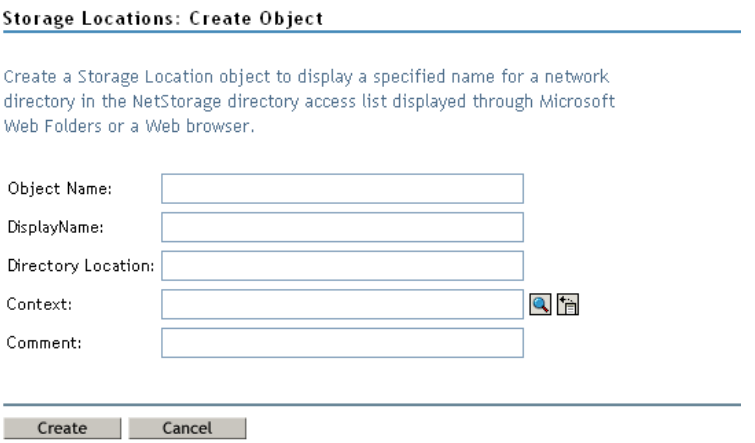
2. Log in to iManager with an administrator ***username*** and **password**.

3. From the left, expand **File Access (NetStorage)**; then select **New Storage Location**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A Storage Locations : Create Object page appears on the right:

Figure 10-6



4. Enter the following:
 - **Object Name.** The name of the object in the eDirectory tree.
 - **DisplayName.** The name displayed in the NetStorage directory access list. This is the shortcut name and is seen by users.

 If you use the same display name for two different Storage Location objects, a digit is added to the names to make each name unique.
 - **Directory Location.** The location of the directory on the file system. The location is a URL that includes the file system type, server name, volume, and directory path.

 If the storage being accessed is on a NetWare server, the URL must be in the following format:

 ncp://*server_name/volume/path_to_directory*

 For example:

 ncp://da2.da.com/data/reports

 or

 ncp://10.200.200.2/data/reports

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If the storage being accessed is on a Linux server, the URL must be in one of the following formats:

- **ncp://*server_name/volume/path_to_directory***

 This method requires that the NCP server component of OES be installed on your Linux server. A storage location using this format can only access files on an NCP or NSS volume.

- **cifs://*server_name/cifs_share_name***

 You can only use this method if you have configured a CIFS or Samba share (cifs can be interchanged with smb in the format).

- **ssh://*yourserver.yourcompany.com/home/youruser***

 This method allows access to files on Linux systems that don't support either NCP or CIFS (SMB) protocols.

If the file system is omitted, it is assumed that it is NCP.

- **Context.** The directory context that the Storage Location object resides in. Use the Object Selector icon (to the right of the field) to select and enter the context.
- **Comment.** You can enter a comment that is not displayed to users.

5. When you finish, select **Create**; then select **OK**.

How to Create a Storage Location List

After you create a Storage Location object, you must create a list of Storage Location objects that can be used with a specified User, Group, Profile, or Container object.

Users will see the directory associated with the object the next time they log in to NetStorage.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

After you create this list, you can modify it in the same window by assigning additional Storage Location objects to the list or by deleting Storage Location objects from the list.

Do the following:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox); then enter the URL for iManager:

 https://*server_ip_address*/nps/iManager

 where ***server_ip_address*** is the IP address or DNS name of the server running NetStorage or the IP address for Apache-based services.

2. Log in to iManager with an administrator ***username*** and ***password***.

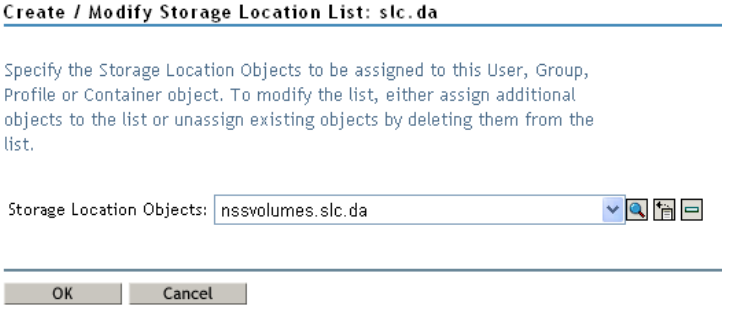
3. From the left, expand **File Access (NetStorage)**; then select **Assign Storage Location to Object**.

4. To the right of the Object field, select the **Object Selector** button.

5. Browse to and select the ***User***, ***Group***, ***Profile***, or ***Container*** object that the list is to be created for; then select **OK**.

 A Create / Modify Storage Location List page appears:

Figure 10-7



6. To the right of the Storage Location Objects drop-down list, select the **Object Selector** button.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

7. Select the ***Storage Location objects*** you want included in this list; then select **OK**.

 You can select multiple Storage Location objects in the Object Selector window. When you select multiple Storage Location objects, they appear in the Selected Objects list.

 If the list already contains Storage Location objects and you want to add more, make sure that the original objects are still in the list before selecting OK.

 You can remove existing storage locations by deleting their names from the list before selecting OK.

8. When you finish, select **OK**.

 An xTier-LocationList attribute (under Other) is added to the User, Group, Profile, or Container object that lists the Storage Locations assigned to the object.

How to Create SSH Storage Location Objects

A new file access method has been added to NetStorage that allows access to files on Linux systems that don't support either NCP or CIFS protocols.

This method uses the Secure Shell (SSH) protocol to access files on Linux systems. SSH is accessed by creating an eDirectory Storage Location object with a URL prefix of ssh://, such as the following:

```
ssh://yourserver.yourcompany.com/home/youruser
```

The username and password that you use to access files on your Linux system must be the same as those used to log in to NetStorage.

You can use the SSH file access method with NetStorage to access files locally on your Linux system if NetStorage is running on that system.

To do this, create a Storage Location object that uses the IP address of the local Linux machine with the ssh:// prefix.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

How to View or Modify Directory and File Attributes and Rights

NetStorage gives you the ability to view or change NSS and NCP directory and file attributes and rights from the NetStorage home page.

If you have created a Storage Location object using NCP, the ability to change file and directory attributes is limited unless you are logged in as user admin or equivalent. This limitation does not apply if you have created a Storage Location object using SSH.

To view or modify directory or file rights from the NetStorage page:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox); then enter the URL for iManager:

 https://*server_ip_address*/nps/iManager

 where ***server_ip_address*** is the IP address or DNS name of the server running NetStorage, or the IP address for Apache-based services.

 If Apache-based services use a port other than 80, you must also specify that port number with the URL.

 For example, if the IP address for NetStorage is 10.200.200.1 and the port number is 51080, then you would enter **https://10.200.200.1:51080/oneNet/NetStorage**.

 A login dialog appears.

2. Enter an eDirectory ***username*** and ***password***.

 NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

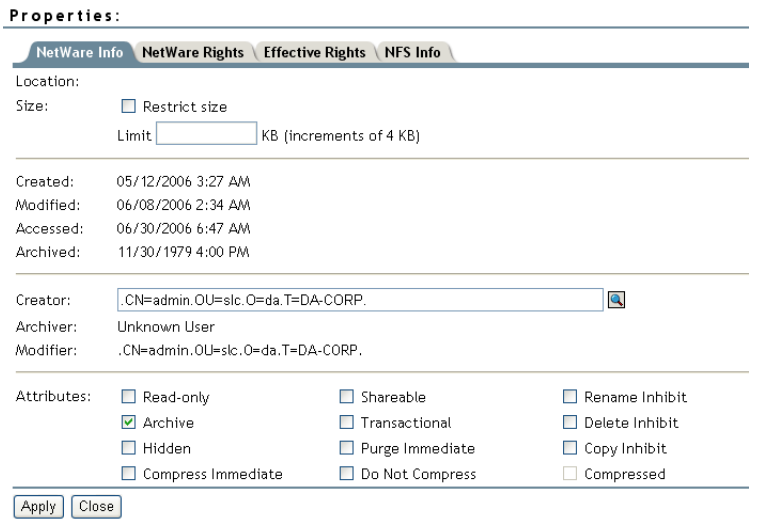
 A NetStorage home page appears.

3. From the right pane, right-click the ***directory*** or ***file*** you want to view or modify attributes or rights for; then select **Properties**.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A Properties page for the directory or file appears:

Figure 10-8



4. View or modify directory or file attributes by selecting the **NetWare Info** tab; view or modify file system trustee rights by selecting the **NetWare Rights** tab.

 Although the tab labels refer to NetWare, you can use the option for your Linux NSS and non-NSS volumes, and your NetWare NSS volumes.



For information about file system trustees, trustee rights, and attributes for directories and files on NSS volumes, see the *Novell Storage Services File System Administration Guide for Novell OES* (nss_enu.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Viewing or changing directory and file attributes and rights using NetStorage is only possible using a browser. This functionality is not available using Microsoft Web Folders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



For information on directory and file attributes and rights, see the *Novell Client for Windows Installation and Administration Guide* (noclenu.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

5. When you finish viewing the Properties information, select **Close**; when you finish making any changes, select **Apply**, and then select **Close**.



If you want to modify file system trustees, trustee rights, and attributes for directories and files when logged in to NetStorage as admin, make sure you assign the admin user to the Storage Location object, or you will not be able to view the directory or file on the NetStorage page when you log in as admin.

How to Set Directory Quotas on NSS Volumes and Directories

From the NetStorage home page, you can create or change directory quotas on NSS volumes and directories for both NetWare and Linux.

You must be a user with rights equivalent to the admin user to create or change directory quotas.

To create or change NSS directory quotas using NetStorage, do the following:

1. Start a supported web browser (such as Internet Explorer or Mozilla Firefox); then enter the URL for iManager:

 https://*server_ip_address*/nps/iManager

 where ***server_ip_address is*** the IP address or DNS name of the server running NetStorage, or the IP address for Apache-based services.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

If Apache-based services use a port other than 80, you must also specify that port number with the URL.

For example, if the IP address for NetStorage is 10.200.200.1 and the port number is 51080, then you would enter **https://10.200.200.1:51080/oneNet/NetStorage**.

A login dialog appears.

2. Enter an eDirectory ***username*** and ***password***.

 NetStorage uses your Novell eDirectory username and password, so you don't need to remember or use a separate username or password.

 A NetStorage home page appears.

3. From the right pane, right-click a ***directory*** or ***file*** you want to view or modify attributes or rights for; then select **Properties**.

 A Properties page appears.

4. Make sure the **NetWare Info** tab is selected; then select (check) the **Restrict size** option.

5. In the Limit field, enter the ***directory size limit***; then save your changes by selecting **Apply**.

6. Close the Properties page by selecting **Close**.

How to Purge and Salvage Deleted NSS Files

From the NetStorage home page, you can purge and possibly undelete NSS files that were previously deleted if either of the following is true:

- You are the admin user and have the NCP server component of OES installed on the Linux server.
- You have a Storage Location object set up for the directory where the deleted files or folders were.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

To purge or salvage delete NSS files from the NetStorage home page, do the following:

1. Access **NetStorage** as the **admin** user.
2. From the left, select the ***directory*** where the deleted files were.
3. Select **View**; then select **Show Deleted Files**.
4. Select (check) the boxes next to the ***files*** you want to undelete or purge.
5. Select File; then select **Purge** or **Undelete**.

NetStorage Implementation Guidelines

The following are some guidelines to help you when implementing NetStorage:

- User and Group Access Rights Assignments
- Access Other Target Systems
- NetStorage Authentication Persistence
- NetStorage Maintenance
- Invalid NetStorage Authentication Domains
- iManager NetStorage Plug-In Options

User and Group Access Rights Assignments

Because NetStorage provides access to other file storage systems, the users and groups that access the other systems through NetStorage must be created and granted file and directory access on those systems.

For example:

- NetWare users must exist in the eDirectory tree where the NetWare server resides and have access rights to the files and directories on the NetWare server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Windows users must exist on the Windows systems and have the required access rights to the files and directories on those systems.
- If your users will access Samba files on an OES Linux server, they must be enabled for LUM and Samba access on the OES Linux server.



The usernames and passwords used to authenticate to the NetStorage (OES) server through eDirectory must match the usernames and passwords defined on the target systems.

Access Other Target Systems

When you install NetStorage (during or after OES installation), you indicate a primary authentication domain (such as slc.da) for NetStorage.

To log in to NetStorage and access storage locations, users must exist somewhere in the context of this primary domain.

When receiving an authentication request, NetStorage searches for the username in the context you specified and in all its subcontexts.

Authentication to other file systems is often controlled by other authentication domains.

For example, you might create a storage location on an OES Linux server that points to a NetWare server that resides in a different eDirectory tree. To access this storage location, users must authenticate to the other tree.

This means that you must specify an additional context in the NetStorage configuration as a nonprimary authentication domain.

When defining a nonprimary authentication domain, you must

- Make sure that the username and password in the nonprimary domain matches the username and password in the primary domain.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Specify the exact context of user objects. NetStorage doesn't search the subcontexts of nonprimary authentication domains.



For details on Authentication Domains, see "Authentication Domains" on page 24 of the *NetStorage Administration Guide for Linux* (netstor_lx.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

NetStorage Authentication Persistence

By default, users must reauthenticate each time they access NetStorage in a browser. This is true even if another browser window is open and authenticated on the same workstation.

The reason for this is that persistent cookies are not enabled by default. This setting can be changed.



For details on persistent cookies, see "Persistent Cookies" on page 28 of the *NetStorage Administration Guide for Linux* (netstor_lx.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

NetStorage Maintenance

Your NetStorage installation can change as your network changes and evolves by providing access to new or consolidated storage locations.

For information about the kinds of tasks you can perform to keep your NetStorage implementation current, see the following:

- For Linux, *OES NetStorage Administration Guide for Linux* (netstor_lx.pdf)

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- For NetWare, *OES NetStorage Administration Guide for NetWare* (netstor.pdf).

Invalid NetStorage Authentication Domains

If you change the default NetStorage Authentication Domain to an invalid domain, either during the OES installation (NetStorage installation) or afterwards with iManager, users may get a blank screen or Service Not Available errors when trying to access NetStorage.

Also, you will not be able to change the Authentication Domains setting to a valid domain using iManager.

If this happens, you can change the Authentication Domains value using the /opt/novell/xtier/bin/xsrvcfg command at the Linux server console. To change the authentication domain value, enter the following command:

LD_LIBRARY_PATH=/opt/novell/xtier/lib /opt/novell/xtier/bin/xsrvcfg -d *authentication_domain* -c authentication_context

Replace ***authentication_domain*** with a valid authentication domain. Replace ***authentication_context*** with a valid authentication context.



For details on authentication domains, see “Authentication Domains” on page 24 of the *NetStorage Administration Guide for Linux* (netstor_lx.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

iManager NetStorage Plug-In Options

The iManager options to manage NetStorage will appear in iManager even if NetStorage is not installed. The NetStorage iManager plug-in is installed even if NetStorage is not. If NetStorage is not installed, the NetStorage iManager options will not be functional.

This also applies if NetStorage and iManager are installed on different servers.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Exercise 10-1 Configure and Use NetStorage

In this exercise, you configure and use NetStorage to allow Digital Airlines employees web access to their server files.

Exercise 10-1 Configure and Use NetStorage is in your *Integrating Novell Open Enterprise Server for Linux Workbook* on page 10-2.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Summary

Objective	Summary
1. Describe the Purpose and Architecture of NetStorage	In order to describe the purpose and architecture of NetStorage, you learned about the following: ■ **What NetStorage provides.** NetStorage provides secure Internet-based access to files and folders on Linux and NetWare servers on your network using either a browser or Microsoft Web Folders (Microsoft's implementation of WebDAV). NetStorage authentication relies on Novell eDirectory to provide secure access, so Internet-based access is as secure as accessing files from within the network. ■ **NetStorage system requirements.** In addition to meeting the requirements for Novell OES, NetStorage requires the following: ■ **Server requirements.** At least one Linux server with OES or one NetWare 6.5 server in the Novell eDirectory tree where NetStorage will be installed. ■ **Workstation requirements.** Netscape Navigator 4.7 or later, Internet Explorer 5.5 or later, Mozilla, Mozilla Firefox, other Linux browsers, or Microsoft Web Folders.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
1. Describe the Purpose and Architecture of NetStorage (*continued*)	■ **Novell NetStorage on OES Linux.** NetStorage on Linux provides local and Web access to files on many systems without requiring the Novell client. ■ **Novell NetStorage on OES NetWare.** NetStorage on NetWare provides local and Web access to files on NetWare and Linux without requiring the Novell client. ■ **How NetStorage works.** NetStorage is installed on one Linux server (or NetWare server) that acts as a Middle Tier (also known as XTier) server. Xtier is Novell's Web services framework and is used by various Novell products. ■ **What users see when they access NetStorage.** The NetStorage web page displays the network files and folders currently accessible for the logged in user.
2. Implement and Manage NetStorage	To perform basic implementation and maintenance tasks on NetStorage, you learned about the following: ■ How to access the NetStorage home page ■ How to administer NetStorage from Novell iManager ■ How to create Storage Location objects and lists ■ How to view or modify directory and file attributes and rights

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
2. Implement and Manage NetStorage (*continued*)	■ How to set directory quotas on NSS volumes and directories ■ How to purge and salvage deleted NSS files ■ About NetStorage implementation guidelines

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

SECTION 11 Plan a Novell OES Implementation

In this section, you review some basic information to help you begin planning and implementing a Novell Open Enterprise Server (OES) solution.

Objectives

As you plan which services to install on which Novell OES platform on your network, you will probably have a number of questions.

The following objectives will help answer your questions and alert you to steps you should follow for a successful Novell OES implementation:

1. Review the Services Included in Novell OES
2. Decide Which OES Platform Is Best Suited to Provide These Services
3. Plan for eDirectory
4. Plan for File Services
5. Plan for Print Services
6. Plan for NetWork Server Usage
7. Review Server Requirements
8. Consider Coexistence and Migration Issues
9. Decide on an Installation Option Before You Start

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Introduction

The previous sections have introduced you to testing Novell OES in a lab environment before introducing it into your network production environment.

Although you were probably familiar with many of the Novell OES services running on NetWare, implementing them in a mixed NetWare and Linux environment creates new challenges that include network communication, configuration, and coexistence issues.

In this section, you review many of these issues in the context of planning for your own implementation of Novell OES.



For additional information about planning a Novell OES implementation, see the *Novell OES Planning and Implementation Guide* (implgde.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 1 Review the Services Included in Novell OES

After working through the exercises in this course, you learned about Novell OES services that you might not have known about.

For example, you learned that the Novell client allows users to map drives to locations on an OES Linux server running the NCP server for Linux.

Beginning with the release of Novell Nterprise Linux Services and expanding with the release of Novell OES, Novell has included Linux versions of many Novell services that have traditionally been available only on NetWare.

In addition, Novell has ported the most well-known, network-critical open source products to NetWare—products such as OpenSSH and the Apache Web server.

The following summarizes the services and technology support available on each platform and the differences in the way these services are provided:

Table 11-1

Service	OES Linux	OES NetWare
Apache Web Server	Yes (standard Linux)	Yes (NetWare port of open source product)
Archive and Version Services	No	Yes
Backup (SMS)	Yes	Yes
Clustering	Yes	Yes
DFS (Distributed File Services)	Yes	Yes
DHCP	Yes	Yes
DNS	Yes	Yes
eDirectory 8.7.3	Yes	Yes

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-1**

Service	OES Linux	OES NetWare
eDirectory Certificate Server	Yes	Yes
eGuide (White Pages)	Yes	Yes
FTP Server	Yes	Yes
Health Monitoring Services	Yes	Yes
Identity Manager	Yes	Yes
iFolder 2.*x*	Yes	Yes
iPrint	Yes	Yes
IPX (Internetwork Packet Exchange)	No	Yes
iSCSI	Yes	Yes
LDAP Server for eDirectory	Yes	Yes
MySQL	Yes (standard Linux)	Yes (NetWare port of open source product)
NCP Server	Yes	Yes
NetStorage	Yes	Yes
NICI (Novell International Cryptography Infrastructure)	Yes	Yes
NMAS (Novell Modular Authentication Services)	Yes	Yes
Novell Client for Windows support	Yes (through NCP Server for Linux or Novell Samba)	Yes
Novell Cluster Services	Yes	Yes

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-1**

Service	OES Linux	OES NetWare
Novell Licensing Services	No	Yes
NSS (Novell Storage Services)	Yes	Yes
Nsure Audit	No	Yes
NTPv3	Yes	Yes
OpenSSH	Yes (standard Linux)	Yes (NetWare port of open source product)
PAM (Pluggable Authentication Modules)	Yes (eDirectory enabled)	No (eDirectory authentication is pervasive on NetWare)
Pervasive.SQL	No (available at http://www.pervasive.com)	Yes
PKI (Public Key Infrastructure)	Yes (eDirectory)	Yes (eDirectory)
RADIUS	Yes (Novell RADIUS)	Yes (Novell RADIUS)
Samba	Yes (Novell customized)	No
Search (QuickFinder)	Yes	Yes
SLP	Yes (SLES 9)	Yes (Novell)
Software RAIDS	Yes (0 and 1)	Yes (0, 1, 5)
Storage Management Services (SMS)	Yes	Yes
TCP/IP	Yes	Yes
Timesync	No	Yes

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-1**

Service	OES Linux	OES NetWare
Tomcat	Yes (Standard Linux)	Yes (NetWare port)
NetWare Traditional File System	No	Yes
Virtual Office (Collaboration)	Yes	Yes



Although extensive, this list does not cover all available services or technologies.

If you are interested in a service or technology that is not listed, or for documentation for listed services, see the “A–Z List” on the OES Documentation web site at http://www.novell.com/documentation/oes.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 2 Decide Which OES Platform Is Best Suited to Provide These Services

To help you better assess which Novell OES platform can best meet your network service needs, you should consider inherent platforms strengths of Linux and NetWare and the differences in the service offerings on each platform.

The following topics help you make this assessment:

- Platform Strengths
- Service Differences on the OES Platforms

Platform Strengths

Although both Novell OES Linux and OES NetWare provide a full set of Novell network services, there are differences the platforms that you need to consider when implementing Novel OES:

Table 11-2

	OES NetWare	OES Linux
Brief description	Novell's award-winning network-optimized operating system.	Novell's award-winning Linux operating system.
Recognized strengths	■ Reliability ■ Scalability ■ Security	■ Open application environment ■ Flexibility ■ Versatility

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-2**

	OES NetWare	OES Linux
Business value propositions (*continued*)	NetWare excels when the user population and management burden is highly distributed: ■ Increases network availability ■ Optimizes manageability ■ Enhances user productivity ■ Runs Apache, Tomcat, MySQL, and other OpenSource applications	SLES 9 is well suited as an application server running Linux-based solutions: ■ Runs thousands of programs available from the open source community ■ Delivers OES file and print services ■ Hosts open source Web servers, proxy servers, and mail servers

Service Differences on the OES Platforms

In addition to considering platform strength, you should understand the following differences in the features available when services are running on OES Linux or OES NetWare:

- **DHS/DHCP.** NetWare DNS/DHCP services are far richer than the basic DNS/DHCP functionality available in the standard Linux implementation.

 Many organizations find Linux DNS/DHCP services to be completely adequate.

 On the other hand, some organizations, especially those that currently leverage the advanced services available on NetWare, might be frustrated with the Linux implementation of DNS/DHCP and find it is inadequate for their needs.

- **Novell Storage Services (NSS).** When deploying NSS, you might want support for volume encryption or Novell Distributed File Services (DFS) so you can move or split NSS volumes.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Both of these features are currently available only on NSS running on NetWare.

You should fully investigate any service differences between platforms before you finalize your service and platform choices.

To help you plan for implementing a production environment deployment of Novell OES, check the service documentation at http://www.novell.com/documentation/oes.

The following indicates which services are the same and which are different. It also shows which services are unavailable on a given platform:

Table 11-3

Service	Availability
Apache Web Server	For information on Apache Web Server, see the following: ■ *Administration Instance Vs. Public Instance on NetWare* (http:// www.novell.com/documentation/oes/web_apache/data/aipcu6x.html#aipcu6x) ■ *What's Different about Apache on NetWare* (http://www.novell.com/documentation/oes/web_apache/data/ail8hvj.html#ail8hvj)
Archive and Version Services	Not supported on Linux.
Backup (SMS)	Available on both platforms with no functional difference.
Clustering	Available on both platforms (designed to run on either an OES Linux cluster or an OES NetWare cluster).
DFS (Distributed File Services)	Not supported in NSS for OES Linux.
DHCP	Available on both platforms with some functional differences.
DNS	Available on both platforms with little functional difference.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-3**

Service	Availability
eDirectory 8.7.3	Available on both platforms with no functional difference.
eDirectory Certificate Server	Available on both platforms with no functional difference.
eGuide (White Pages)	Available on both platforms with no functional difference.
FTP Server	Available on OES NetWare only. See “Features of the NetWare FTP Server” on page 10 of the *Novell OES NetWare FTP Server Administration Guide* (ftp_enu.pdf).
Identity Manager	Available on both platforms with no functional difference.
iFolder 2.*x*	Available on both platforms with no functional difference.
iPrint	Available on both platforms with some functional differences.
IPX (Internetwork Packet Exchange)	Not available on Linux.
iSCSI	Available on both platforms (see the Linux-iSCSI Project at http://linux-iscsi.sourceforge.net).
LDAP Server for eDirectory	Available on both platforms with no functional difference.
MySQL	Available on both platforms (see MySQL.com on the web at http://www.mysql.com).
NCP Server	Available on both platforms with no functional difference.
NetStorage	NetStorage on Linux offers connectivity to storage locations using the CIFS/SMB, NCP, and SSH protocols. NetWare uses only NCP.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-3**

Service	Availability
NICI (Novell International Cryptography Infrastructure)	Available on both platforms with no functional difference.
NMAS (Novell Modular Authentication Services)	Available on both platforms with no functional difference.
Novell Client for Windows support	No functional differences with NCP Server for Linux installed on OES Linux.
Novell Cluster Services	Available on both platforms with no functional difference.
Novell Licensing Services	Not available on Linux.
NSS (Novell Storages Services)	Available on both platforms with some functional differences. See “Comparison of NSS on NetWare and NSS on Linux” on page 285 in the *Novell OES Novell Storage Services File System Administration Guide* (nss_enu.pdf). You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.
Nsure Audit	Not available on Linux.
NTPv3	Available on both platforms. See “Time Synchronization” on page 169 of the *Novell OES Planning and Implementation Guide* (implgde.pdf). You can access the guide from http://www.novell.com/documentation or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-3**

Service	Availability
OpenSSH	Available on both platforms with little functional difference. See “Functions Unique to the NetWare Platform” on page 10 in the *Novell OES OpenSSH Administration Guide for NetWare* (openssh.pdf). You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.
PAM (Pluggable Authentication Modules)	Not supported on NetWare. Authentication is fully integrated with eDirectory.
Pervasive.SQL	See Pervasive.SQL on the web (http://www.pervasive.com/support/technical/online_manuals.asp).
PKI (Public Key Infrastructure)	Available on both platforms with no functional difference.
RADIUS	Available on both platforms with no functional difference (NMAS).
Samba	This is a Linux solution. NetWare has Native File Access Protocol Support.
Search (QuickFinder)	When indexing a file system, the QuickFinder engine only indexes what it has rights to see. On NetWare, it has full access to all mounted volumes. On Linux, it has rights to only the files that the novelwww user in the www group has rights to see. For more information, see “Security Characteristics” on page 156 and “Generating an Index For a Linux-mounted NSS Volume” on page 81 in the *Novell QuickFinder Server 4.2 Administration Guide* (qfserver.pdf).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-3**

Service	Availability
Search (QuickFinder) (*continued*)	You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.
Server resource management (eDirectory)	eDirectory on NetWare manages server resources. For example, you can view and modify file system information, manage files and folders on NetWare volumes, salvage and purge deleted files, allocate volume space, and create objects to facilitate file management. See “Managing Objects” on page 87 in the *Novell eDirectory 8.7.3 Administration Guide* (edir873.pdf). You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*. The current version of eDirectory for Linux does not support management of server resources.
SLP	Available on both platforms with some functional differences. OES Linux uses OpenSLP. OES NetWare uses Novell SLP by default, which provides synchronization between DAs that are in the same eDirectory context. Alternatively, you can implement OpenSLP for eDirectory. Be aware, however, that DA synchronization is not supported in OpenSLP. OpenSLP on Linux is not customized to provide DA synchronization.
Storage Management Services (SMS)	Available on both platforms with no functional difference.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-3**

Service	Availability
TCP/IP	Available on both platforms with no functional difference.
Timesync	Not available on Linux.
Tomcat	Available on both platforms with some functional differences. See “Administration Instance vs. Public Instance of Tomcat on NetWare” on page 10 of the *Novell OES Tomcat for NetWare Administration Guide* (web_tomcat.pdf). You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.
NetWare Traditional File System	Not available on Linux.
Virtual Office (Collaboration)	Available on both platforms with no functional difference.
WAN Traffic Manager	Not supported on Linux. See “WAN Traffic Manager” on page 229 in the *Novell eDirectory 8.7.3 Administration Guide*. You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 3 Plan for eDirectory

eDirectory is the heart of OES's powerful network services and security.

If you are installing an OES server into an existing tree, be sure you understand the information in "eDirectory Coexistence and Migration" on page 81 of the *Novell OES Planning and Implementation Guide* (implgde.pdf).



You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

If you are creating a new eDirectory tree on your network, you must do some additional planning before you install the first server into the tree. The first server is important for two reasons:

- You create the basic eDirectory tree structure during the first installation.
- The first server permanently hosts the Certificate Authority (CA) for your organization.

To ensure that your eDirectory tree meets your needs, take time to plan the following:

- **Structure of the eDirectory tree.** A well-designed tree provides containers for items such as servers, users, and printers. It is also optimized for efficient data transfer between geographically dispersed locations.



For more information, see "Designing Your Novell eDirectory Network" on page 67 in the *Novell eDirectory 8.7.3 Administration Guide* (edir873.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **Time synchronization.** eDirectory requires that all OES servers, both NetWare and Linux, be time synchronized.
- **Partitions and replicas.** eDirectory allows the tree to be partitioned for scalability. Replicas (copies) of the partitions provide fault tolerance within the tree.

 The first three servers installed into an eDirectory tree automatically receive replicas of the tree's root partition. You might want to create additional partitions and replicas.



For more information, see "Managing Partitions and Replicas" on page 113 in the *Novell eDirectory 8.7.3 Administration Guide* (edir873.pdf).

You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

If you are installing OES into an existing tree (installed before NetWare 6.5), you must be sure to prepare the network using Deployment Manager (located on *Novell OES NetWare Installation CD1*).

If you want to create a new eDirectory tree that will contain both NetWare and Linux servers, you must start the tree creation using a NetWare server first.

If you use a Linux server to create a new tree and subsequently add a NetWare server to the newly created tree, you will not be able to install any client or server licenses.

Any features that require either a NetWare server license or NetWare Client access license will be inaccessible.



This issue will be addressed in a future release of Novell OES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 4 Plan for File Services

To decide which file service components to install, you should match service features listed in the following to your network's file service requirements:

Table 11-4

Product	Features
iFolder	**Access method features** ■ Linux file managers ■ Offline access with file synchronization (between local and network copies) on reconnect ■ Windows Explorer **Back-end storage features** ■ iFolder file repository on OES server **Security features** ■ Files encrypted on the iFolder server and for transport ■ Secure LDAP authentication
Native File Access Protocol (NFAP) (NetWare only)	**Access method features** ■ Linux file managers ■ Macintosh Finder ■ UNIX file managers ■ Windows Explorer **Back-end storage features** ■ NetWare volumes **Security features** ■ Secure LDAP authentication

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-4**

Product	Features
NCP (NetWare Core Protocol) Server	**Access method features** ■ Novell Client (NCP client) **Back-end storage features** ■ Any Linux volumes, including NSS, that are defined as NCP volumes ■ NetWare volumes **Security features** ■ eDirectory authentication
NetStorage	**Access method features** ■ Any supported browsers ■ Personal Digital Assistants (PDAs) ■ Remote (browser-based) ■ Web folders (in Internet Explorer or in Windows Explorer) ■ Windows Explorer **Back-end storage features** ■ iFolder server (on same machine) ■ Linux traditional volumes ■ NetWare volumes ■ NCP volumes ■ NSS volumes ■ Samba (SMB) servers ■ Windows (CIFS) servers NetStorage only provides access to other file services. **Security features** ■ Secure LDAP authentication

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-4**

Product	Features
Novell Samba (Linux only)	**Access method features** ■ Any CIFS/SMB client ■ Remote access (Web folders in the Internet Explorer browser) ■ Windows Explorer **Back-end storage features** ■ Linux traditional file system on OES server **Security features** ■ Secure LDAP authentication

To plan for your OES file services, do the following:

1. For the file services you plan to install, compute the total additional RAM required (above the basic system requirement).

 Refer to the following points for help:

 - **iFolder.** For suggestions on calculating the additional RAM, see "Preparing to Install iFolder 2.1" on page 25 in the *Novell iFolder 2.1 Installation and Administration Guide* (admin.pdf).



You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

 - **Native File Access Protocols.** There are no additional RAM requirements.
 - **NCP.** There are no additional RAM requirements.
 - **NetStorage.** There are no additional RAM requirements.
 - **Samba.** There are no additional RAM requirements.

2. Record the additional RAM requirements in your planning notes.
3. For the file services you plan to install, compute the total additional disk space required (above the basic system requirement).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Refer to the following points for help:

- **iFolder.** For suggestions for calculating the additional disk space you will need see "Preparing to Install iFolder 2.1" on page 25 in the *Novell iFolder 2.1 Installation and Administration Guide* (admin.pdf).



You can access the guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

- **Native File Access Protocols.** You should allocate enough disk space to meet your users' file storage needs.

 Because all platforms can access the same storage space, you only need to consider the total space needed, not the platform-specific requirements.

- **NCP.** You should allocate enough disk space to meet your users' file storage needs.

 On Linux, this space must exist on partitions you have designated as NCP volumes. On NetWare, all volumes are accessible through NCP.

- **NetStorage.** There are no disk space requirements because NetStorage provides access to other file storage services; it doesn't provide storage services.

- **Samba.** You should allocate enough disk space for the partition containing the /home directory to meet your users' file storage needs.

4. Record the additional disk space requirements in your planning notes.

5. For the file services you plan to install, refer to the information in this section and the OES installation guides (at http://www.novell.com/documentation/oes) and note your planning choices on your planning sheet.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 5 Plan for Print Services

Use the following to help you plan your iPrint installation:

- We recommend you record your planning decisions on a planning worksheet for future reference.
- iPrint has no additional RAM requirements.
- Most iPrint installations (even in large enterprises) do not require additional disk space for associated print job spooling.

 However, if you anticipate very heavy print usage and want to plan for additional disk space, the iPrint spooler area is located in the /var partition or directory structure on OES Linux servers.

 On NetWare servers you designate the location when creating the Print Manager object.
- To finish planning your iPrint installation, refer to the information for your server platform:
 - For NetWare, see "Novell iPrint Server" on page 46 in the *Novell OES Installation Guide for NetWare* (install-nw.pdf).
 - For Linux, see "Novell iPrint" on page 43 in the *Novell OES Installation Guide for Linux* (install-linux.pdf).



You can access these guides from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 6 Plan for NetWork Server Usage

To effectively use your network servers for a Novell OES deployment, you need to do the following:

- Identify a Purpose for Each Server
- Review Server Requirements
- Consider Coexistence and Migration Issues

Identify a Purpose for Each Server

Large networks usually have one or more servers dedicated to providing a single network service.

For example, one or more servers might be designated to provide iFolder file services to network users while other servers provide iPrint printing services for the same users.

For smaller organizations, it is often not practical or cost-effective to dedicate servers to providing a single service. For example, the same server might provide both file and print services to network users.

Prior to installing a new server on your network, you should identify the service or services that it will provide.

Review Server Requirements

OES Linux and OES NetWare both have specific hardware and software requirements.

Before installing OES, make sure your server machine and network environment meet the requirements outlined in the following manuals:

- **OES Linux.** See “Preparing to Install OES Linux” on page 13 in the *Novell OES Installation Guide for Linux* (install-linux.pdf).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- **OES NetWare.** See "Meet Hardware and Software Requirements" on page 13 in the *Novell OES Installation Guide for NetWare* (install-nw.pdf).



You can access these guides from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Consider Coexistence and Migration Issues

You probably already have a network that provides services to network users. In many cases the services you are currently running will influence your approach to implementing Novell OES.

In some cases, there are specific paths to follow so that the Novell OES integration process is as smooth as possible.

Novell has invested considerable effort in identifying service coexistence and migration issues you might face. However, we can't anticipate every combination of services that you might have.

Therefore, we intend to continue developing coexistence and migration information even after the initial Novell OES product releases, and we plan to update the web-based documentation regularly with the newly developed information.

For information about coexistence of Novell OES servers with existing NetWare and Linux networks, and for migration instructions, see the *Novell OES Coexistence and Migration Guide* (coexist-mig.pdf).



You can access this guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective 7 Decide on an Installation Option Before You Start

Before installing Novell OES, you might want to be aware of the following information:

- Installation from CDs or from the Network
- Pattern Deployments
- Installing NSS on a Single-Drive Server

Installation from CDs or from the Network

Both OES Linux and OES NetWare can be installed from CDs or from files on the network:

- **OES Linux options.** OES Linux includes two installation options, both of which are documented in the *Novell OES Installation Guide for Linux* (install-linux.pdf):
 - **CD installation.** You can install using CDs obtained from a Novell Authorized Reseller, or you can create CDs from downloaded ISO image files.

 See “Preparing for a CD Install” on page 26 in the *Novell OES Installation Guide for Linux*
 - **Network installation.** You can install using only the first CD if the remaining ISO files are available on the network.

 This option can save you from swapping CDs on the server during the installation.

 See “Preparing for a Network Install” on page 24 in the *Novell OES Installation Guide for Linux*.
- **OES NetWare options.** OES NetWare includes two installation options, both of which are documented in the *Novell OES Installation Guide for NetWare* (install-nw.pdf):
 - **CD installation.** You can install using CDs obtained from a Novell Authorized Reseller, or you can create CDs from downloaded ISO image files.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

See “Access the Installation Files” on page 30 in the *Novell OES Installation Guide for NetWare*.

- **Network installation.** You can install from the network if you have prepared the DOS partition with Novell Client software and copied the CD files to the network.

 This option can save you from swapping CDs on the server during the installation.

 See “Access the Installation Files” on page 30 in the *Novell OES Installation Guide for NetWare*.



You can access these guides from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Pattern Deployments

Both Novell OES platforms include patterns—server installation options that install only the components required to provide a specific set of network services.

For example, if you want to install n Novell OES server that supports a web-based, user-configurable collaboration environment, you should select the Virtual Office Server pattern during the Novell OES installation.

You should always choose a pattern installation if one fits the intended purpose of your server. If none of the patterns fit, you can install a customized Novell OES server with the service components you need.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following OES Linux installation patterns are available:

Table 11-5

Server Pattern	Description and Packages Installed
Novell Quick Finder Server	Installs a search server that lets users find the information they're looking for on Web sites and attached file systems. KDE is not installed.
Novell iFolder2 Server	Installs a server that lets mobile users access their local files from anywhere—online, offline, all the time. KDE is not installed.
Novell Virtual Office Server	Installs a collaboration solution that lets users be self-sufficient with their IT needs. KDE is not installed.
Novell Management Server	Installs iManager, YaST (text-based), and the basic runtime system. KDE and graphical base system are not installed.
Novell Print Server	Installs a printing system that installs workstation print drivers and gives access to local printers and remote printers with Internet connections. KDE is not installed.
Novell Open Enterprise Server	Installs the SLES 9 default installation and most OES services (default server pattern). KDE is installed.

The following OES NetWare installation patterns are available:

Table 11-6

Server Pattern	Description and Packages Installed
Customized NetWare Server	Lets you select the optional products you want on the server.
Basic NetWare File Server	Installs only basic NetWare with no additional products.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-6**

Server Pattern	Description and Packages Installed
Pre-Migration Server	Creates a server that data will be migrated to at a later time using the NetWare Migration Wizard.
DNS/DHCP Server	Sets up the Novell eDirectory tree for directory-enabled DNS and DHCP services.
exteNd J2EE Web Application Server	Installs an optimized configuration of the Novell exteNd Application Server.
LDAP Server	Installs Lightweight Directory Access Protocol (LDAP) Services for Novell eDirectory.
NetWare AMP (Apache, MySQL, PHP, and Perl) Server	Lets you host open source Web database applications on a NetWare 6.5 server.
NetWare Backup Server	Installs the infrastructure for backup and restore services on the NetWare platform.
QuickFinder Server	Installs a search server that lets users find the information they're looking for on Web sites and attached file systems.
Network Attached Storage (NAS) Server	Installs multiple-file protocol storage for your network.
Novell iPrint Server	Installs a printing system that installs workstation print drivers and gives access to local printers and remote printers with Internet connections.
Apache/Tomcat Server	Installs Apache Web Server and the Jakarta-Tomcat Servlet Container for use in hosting dynamic, application-driven web sites.
Novell Nsure Audit Starter Pack Server	Installs the centralized auditing service that is built into OES NetWare.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table 11-6**

Server Pattern	Description and Packages Installed
iSCSI SAN Storage Server	Turns your OES NetWare server into an iSCSI Storage Server (also known as an iSCSI Target).
Novell iFolder Storage Services	Installs a server that lets mobile users access their local files from anywhere—online, offline, all the time.
Management Server	Installs Novell iManager 2.5 and Novell ConsoleOne 1.3.6 network administration software to provide a complete management solution for your server environment.
Virtual Office Server	Installs a collaboration solution that lets users be self-sufficient with their IT needs.

Installing NSS on a Single-Drive Server

Many organizations are very interested in Novell Storage Services (NSS) running on OES Linux.

If you plan to experiment with NSS on a single-drive server, be sure to follow the instructions in "Installing Linux with EVMS as the Volume Manager of the System Device" on page 117 in the *Novell OES Installation Guide for Linux*.



You can access this guide from http://www.novell.com/documentation/oes or from the OES_Docs directory on your *3077 Course CD*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Summary

Objective	Summary
1. Review the Services Included in Novell OES	Beginning with the release of Novell Nterprise Linux Services and expanding with the release of Novell OES, Novell has included Linux versions of many Novell services that have traditionally been available only on NetWare. In addition, Novell has previously ported the most well-known, network-critical open source products to NetWare—products such as OpenSSH and the Apache Web server. In this objective, you reviewed a summary of the services and technology support available on each platform and the differences in the way these services are provided
2. Decide Which OES Platform Is Best Suited to Provide These Services	To help you better assess which Novell OES platform can best meet your network service needs, you should consider inherent platforms strengths of Linux and NetWare and the differences in the service offerings on each platform. In this objective, you learned the following to help you make this assessment: ■ Platform Strengths ■ Service Differences on the OES Platforms

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
3. Plan for eDirectory	If you are creating a new eDirectory tree on your network, you must do some additional planning before you install the first server into the tree. In this objective, you learned about considerations such as time synchronization and eDirectory tree structure.
4. Plan for File Services	To decide which file service components to install, you learned how to match service features (such as iFolder and NetStorage) to your network's file service requirements.
5. Plan for Print Services	In this objective, you learned about several guidelines that help you plan your iPrint installation.
6. Plan for NetWork Server Usage	To effectively use your network servers for a Novell OES deployment, you need to do the following: ■ Identify a Purpose for Each Server ■ Review Server Requirements ■ Consider Coexistence and Migration Issues

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Objective	Summary
7. Decide on an Installation Option Before You Start	In this objective, you learned that before installing Novell OES, you might want to be aware of the following information: ■ Installation from CDs or from the Network ■ Pattern Deployments ■ Installing NSS on a Single-Drive Server

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

APPENDIX A eDirectory Fundamentals

In this appendix, you are introduced to some fundamental eDirectory concepts you might need to know to help you understand what you are doing when completing the exercises in the *Integrating Novell Open Enterprise Server for Linux* course.

These fundamentals include the following topics:

- Purpose and Function of a Directory
- The Role and Benefits of eDirectory
- eDirectory Components
- eDirectory Object Classes
- eDirectory Object Context and Naming Conventions
- Components of a Solid eDirectory Foundation

If you are already familiar with eDirectory, you can use these topics as a reference when completing the exercises. If you are new to eDirectory, we suggest you take the time to read through the topics before starting the course.



These topics are from the *Fundamentals of Novell eDirectory* course (Course 3017). If you feel you need additional training in eDirectory fundamentals, you might want to attend a 3017 course or purchase the self-study student kit.

For details on the self-study kit, see http://www.novell.com/training/selfstudy.html. For information on available classes, see http://www.novell.com/training/train_product/.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Purpose and Function of a Directory

In this part of the appendix, you learn the following about a Directory:

- What Is a Directory?
- Describe the Purpose of a Directory
- Identify Common Directory Service Uses
- Identify Key Components of a Basic Directory

Most people are familiar with directory services such as the telephone directory. Telephone companies provide a directory of their subscribers' names, addresses, and phone numbers that allows telephone service users to easily contact each other.

All the contact information is in one place—the phone book—which organizes the information in alphabetical order.

Similarly, a network Directory service provides the location of network resources, such as file servers, printers, and applications. This allows network service users and administrators to easily connect to and use or manage these network resources.

All the network resource information is in one place—the Directory tree—which organizes the physical network into a logical network representation.

What Is a Directory?

A Directory is a compilation of services that provide discovery, security, storage, and relationship management.

A Directory should do the following:

- Enable access to resources on the entire network and not just specific servers
- Provide secure access to network resources

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

- Provide a scalable, indexed, and cacheable database (for performance)
- Manage relationships between directory entities, such as users and the resources they access

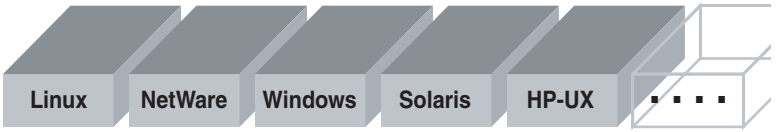
Describe the Purpose of a Directory

Networking provides the ability to share resources. A Directory service gives users a way to locate those shared resources.

A Directory is implemented on a network operating system (NOS). In most cases, users don't need to know the operating system behind the resources they access.

System administrators, however, need to know how to communicate with the various operating systems, maintain current information accurately, and make all operations transparent to the user.

Figure A-1



In an organization, you might find one or more NOS's being used. As business organizations interact and share information, additional NOS's may need to interact. Communication across these systems then becomes the key to success.

To accomplish this task, you need to look beyond current networking infrastructure and identify the tools needed to connect a network with other resources.

A Directory should be able to provide an enterprise-wide solution for this problem.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Identify Common Directory Service Uses

A full-service Directory is typically used in the following ways:

- **To organize data.** A Directory service is an organized listing of data or information. eDirectory stores information about users, servers, printers, and other network devices.

 This helps network administrators perform their jobs better.

- **To more provide easy access to information.** A Directory service makes information about network resources available to users, devices, or applications.

 Directory services give users global access to network resources. Directory services also help organizations manage large numbers of mobile users.

 Some network applications that need access to user information use a Directory to store this information. These applications are called *Directory-enabled*.

 A Directory service is useful because it provides a comprehensive and logical list of all network resources, such as users, applications, services, system resources, and devices.

- **To provide security.** Organizations also use Directory services to provide user authentication to network resources, and authorize users to access specific network resources and services.

- **To provide services to customers.** Hospitals, e-businesses, and other industries use Directory services to provide service to customers.

 The power of the Directory service helps businesses lay the foundation for e-business by

 - Putting their multiple databases in order
 - Simplifying disparate networks
 - Allowing better management of processes between customers, employees, and supply-chain partners

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Other services provided by Directory-enabled products include automated provisioning, enhanced security, customer profiling, electronic wallets, automated notification systems, customized web interfaces, and virtual private networks (VPNs).

Identify Key Components of a Basic Directory

With the global direction of today's economy and business practices, it is logical and necessary that Directories, at least in their basic structural form, follow certain standards.

X.500 is an International Organization for Standardization (ISO) and International Telecommunication Union (ITU) standard that globally defines how Directory services ought to be structured at the basic level.

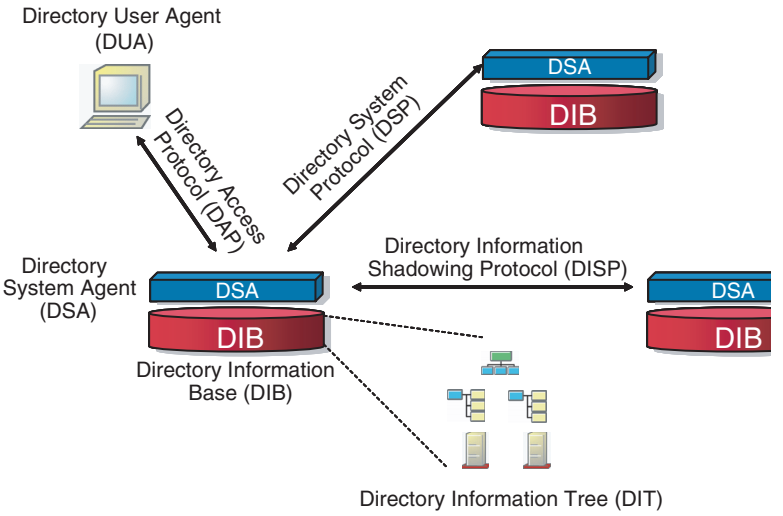
Novell eDirectory, as a leading eBusiness solution, conforms to several key defining components of the X.500 standard.

To effectively understand and manage eDirectory in your network, you need to understand the components of the X.500 Directory.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The following illustrates the components of the X.500 Directory:

Figure A-2



The X.500 Directory standard has seven essential components:

- Directory Information Database (DIB)
- Directory Information Tree (DIT)
- Directory User Agent (DUA)
- Directory System Agent (DSA)
- Directory Access Protocol (DAP)
- Directory System Protocol (DSP)
- Directory Information Shadowing Protocol (DISP)

Directory Information Database (DIB)

A Directory is made up of objects that represent physical resources in the real world. For example, people, servers, and printers are represented by objects in the Directory tree.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Collectively, these objects are known as the Directory Information Database (DIB).

Each object, or entry, in the DIB has a distinguished name that uniquely identifies it. Each entry consists of one or more attributes and each attribute has a value.

In eDirectory, the DIB is designed to be distributed on DSAs across the network. Unless the network is very small, the entire DIB does not exist on any one DSA in the network. The DIB should be logically partitioned, with different partitions residing on different DSAs.

Directory Information Tree (DIT)

The Directory Information Tree (DIT) is a tree structure that logically represents and describes the collection of objects and the relationship of information in the DIB.

The objects are contained in a hierarchical arrangement in this tree structure.

For example, a person (object/entry) works for a company (object/entry) that is located within a country (object/entry).

To keep the Directory organized, a set of rules is enforced to ensure that the DIB remains stable and intact as modifications are made to it over time.

These rules are known as the Directory schema. They prevent entries from having the wrong attribute type or objects from being members of the wrong object classes.

Directory User Agent (DUA)

The X.500 specification uses a client/server approach in communicating information. The client interacts with a server to perform specific Directory operations.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The Directory User Agent (DUA), acting as the client, is an application process that represents each user accessing the Directory. Users are people or programs that can read, modify, or search the Directory.

The DUA requests information from the Directory and then relays that information to the user or program.

Directory System Agent (DSA)

The Directory System Agent (DSA) is the server side of the client/server relationship.

The DSA takes a request from a DUA, services the request, and sends replies to the DUA. If it doesn't have the requested information, it will pass the request on to another DSA.

The DSA consists of many different pieces, including components that communicate with other DSAs on behalf of a DUA and components that are responsible for replication of data between DSAs.

In eDirectory, each DSA holds a master copy or replicated copy of one or more of the DIB partitions.

Directory Access Protocol (DAP)

Directory Access Protocol (DAP) is the protocol that a DSA uses when it communicates with a DSA to make a request of the DSA.

The APIs used to access eDirectory and the Lightweight Directory Access Protocol (LDAP) are examples of a DAP.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Directory System Protocol (DSP)

If a DSA cannot fulfill the request of a DUA, the DSA passes the request to another DSA. The Directory System Protocol (DSP) provides the communication between the two DSAs.

Directory Information Shadowing Protocol (DISP)

The DIB (or partition of the DIB) should be replicated to other DSAs. This improves the performance of requests made to the Directory and provides fault tolerance with a secondary (or backup) copy of the DIB.

In eDirectory, the process of distributing the DIB is called *replication*; in the X.500 specification, it is called *shadowing*. The Directory Information Shadowing Protocol (DISP) performs the actual exchange of replicated information between DSAs.

In eDirectory, replication of DIB partitions is one of the administrator's most important tasks.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The Role and Benefits of eDirectory

Novell eDirectory is the foundation for the world's largest identity management deployments—a high-end Directory service that allows businesses to manage identities and security access for employees, customers, and partners.

With eDirectory, businesses lay the groundwork for secure identity management solutions and multiplatform network services.

As companies increase their presence in the global market and incorporate more networks with multiple platforms, a scalable and diversity-friendly Directory is needed.

You should become familiar with the following:

- The Role of eDirectory
- The History of eDirectory
- eDirectory Features
- eDirectory Platform Support
- The eDirectory Database
- eDirectory Application Support

The Role of eDirectory

Novell eDirectory is a secure identity management solution that runs across multiple NOS platforms. It is Internet-scalable and extensible.

eDirectory is a hierarchical, distributed database that provides the basic foundation for the Directory service, along with replication and partitioning capabilities.

Companies use eDirectory as a means of managing users and all their network hardware and applications.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The role of eDirectory is to provide the basic foundation for the Directory service. This foundation provides replication and partitioning capabilities, along with other utilities. It also provides the following benefits:

- Central management of network information, resources, and services
- A standard method of managing, viewing, and accessing network information, resources, and services
- A logical organization of network resources that is independent of the physical characteristics or layout of the network
- Dynamic mapping between an object and the physical resource it refers to

The History of eDirectory

NetWare Directory Services® (NDS®) was introduced with the release of NetWare® 4.

As Directory services expanded from the local area network to the enterprise-wide area network, and then finally to the Internet, it became necessary for the Directory to be scalable and to be faster.

When NDS 8 was introduced, a new fast and highly scalable database was implemented.

The new Directory was renamed eDirectory because of its scalability and business-to-business enhancements. As the Directory has matured, it has moved to additional platforms. The eDirectory version is now the same across all platforms.

eDirectory is the most powerful cross-platform Directory in the industry.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

eDirectory Features

eDirectory does the following:

- Provides centralized identity management infrastructure
- Supports open and emerging standards
- Enforces network-wide security dynamically
- Incorporates a flexible security framework
- Provides failover and disaster recovery
- Scales to more than one billion identities
- Manages all identities, resources, devices, and policies
- Offers complete Web-based administration

Some of the latest eDirectory features include

- Updated administration utilities
- New backup and restore tool
- Additional platform support

eDirectory Platform Support

eDirectory can be implemented on the following platforms:

- Linux
- NetWare
- Solaris
- Tru64 UNIX
- Windows NT/2000/2003



For complete system requirements, see http://www.novell.com/products/edirectory/sysreqs.html.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The eDirectory Database

eDirectory uses a highly scalable indexed database, called the Flexible Adaptable Information Manager (FLAIM) database, instead of a fixed-length record data store. It uses log files to back out and roll forward transactions in the event of a system failure.

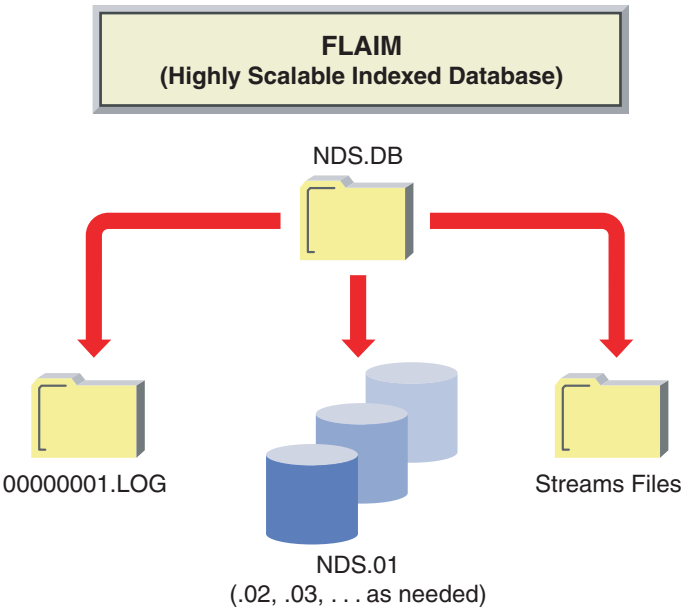
The FLAIM database also provides scalability by limiting the size of database files and automatically creating additional database files when necessary (see Figure A-3).

Even though a Directory is a collection of information, it does not replace traditional Relational Database Management Systems (RDBMS). These are two different entities with different functions.

Directories and databases complement one another. Directories and databases serve different purposes and each is optimized for its respective tasks.

Some of the files that comprise the eDirectory database are shown in the following:

Figure A-3



Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The eDirectory database files are described below:

- **NDS.DB** is the control file for the database. This file contains the roll-back log, which is used to abort incomplete transactions.
- **00000001.LOG** tracks transactions that have not been completed. eDirectory uses this file as a roll-forward log to reapply completed transactions that might not have been fully written to disk because of a system interruption.

 The roll-forward log-naming convention starts with 00000001.LOG and, as needed, increments to FFFFFFFF.LOG.

 These files are used with the eDirectory Backup and Restore tool, covered later in this course.
- **NDS.01** is the main eDirectory database file. It contains all records and indexes found on the server.

 When this file reaches 4 GB, NDS.02 is created for the remaining data. NDS.03, NDS.04, etc., are created as necessary.

 Limiting NDS.*xx* files to 4 GB allows the database to remain scalable yet quickly accessible.

 A number of indexes are maintained in the NDS.01 file, greatly enhancing performance.

 The total database size can grow into terabytes.
- **Stream files** are named with hexadecimal characters (0–9, A–F) and hold information such as print job configurations and login scripts. Stream files have an .nds extension.

eDirectory Application Support

Additional products that build on this basic Directory structure from Novell and Novell partners are also available. These products fall into the following categories:

- Licensed Novell Products
- Partner eDirectory Products

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Licensed Novell Products

Licensed Novell products that leverage eDirectory to provide collaboration, network resource management, network security, and identity management include

- GroupWise®
- ZENworks®
- BorderManager®
- Novell Account Management
- Novell Identity Manager (formerly DirXML™)

Partner eDirectory Products

Partners have developed many different products to leverage the power of eDirectory.

To see what other products work with eDirectory, visit http://www.novell.com/partnerguide/workswith.html and select the **eDirectory** link from the list on the right.

A searchable product database is available to help you locate the product you are looking for.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

eDirectory Components

eDirectory consists of a hierarchical tree structure that stores and organizes objects. The *schema* defines the objects, properties, and values that can be placed in the tree. The following are explained in more detail:

- Tree
- Schema
- Objects
- Properties
- Values
- Object Example

Tree

The *eDirectory tree* is a hierarchical structure (as shown in Figure A-4) that stores and organizes objects. It includes the tree object and container objects.

The eDirectory tree lets you view the logical organization of network resources in the Directory database.

Schema

The *schema* defines the types of objects that can be created in your tree (such as users, printers, and groups) and what information is required or optional at the time the object is created.

The schema that originally shipped with the product is called the *base schema*. If you modify the base schema in any way, it is considered an *extended schema*.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Many Novell products, such as iFolder, ZENworks, and GroupWise, extend the schema during installation, by adding object classes and attributes that make it possible to manage the products through eDirectory.

For example, iFolder adds the iFolder server object.

Objects

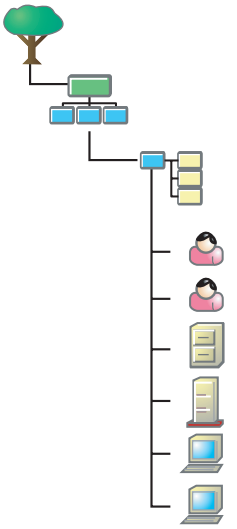
An *object*, also referred to as an *entry*, is a unit of information about a resource, comparable to a record in a conventional database. eDirectory represents each network resource as an object in the Directory.

Different types or categories of objects exist.

An object can be a physical resource (workstation), an eDirectory resource (group), or an organizational resource (container).

The following shows common eDirectory objects:

Figure A-4



Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Properties

A *property*, also referred to as an *attribute*, is a category of information you can store about an object. Each eDirectory object consists of properties that can be used to store information about the resource.

A particular collection of properties defines or makes up the class of an object. For example, a workstation object differs from a user object in the properties it contains and, therefore, in how the object can be used.

Workstation objects do not have a username like a user object. Workstation objects cannot belong to group objects or role objects like a user object can.

Object classes and properties are defined and controlled by the eDirectory schema.



The terms *object* and *property* are used when referring to the hierarchical structure of eDirectory. The term *entry* and *attribute* are sometimes used interchangeably with object and property and typically refer to the underlying database.

Values

A *value* is the data within a property.

For example, a user object has an attribute, or property, called Last Name, which in turn has a value, such as Johnson.

Object Example

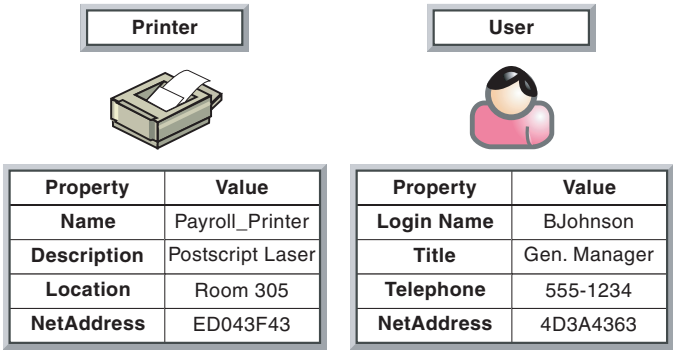
In the following figure, a printer is represented by a printer object. The properties associated with the printer object include Name, Description, and Location. The values for these properties are Payroll_Printer, PostScript Laser, and Room 305, respectively.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A user is represented as a user object. Like the printer object, the user object has properties associated with it. These properties include Login Name, Title, and Telephone.

All eDirectory objects, like the printer object and user shown in the following, have properties and values:

Figure A-5



Property	Value
Name	Payroll_Printer
Description	Postscript Laser
Location	Room 305
NetAddress	ED043F43

Property	Value
Login Name	BJohnson
Title	Gen. Manager
Telephone	555-1234
NetAddress	4D3A4363

Note that the user object also has properties and values. However, because a user object performs a different function, its properties and values are different.



When you create a user object in iManager, the Last Name property is referred to as Surname. However, when you open a user object's General property page, you see the Surname property referred to as Last Name.

Object properties fall into two categories:

- Mandatory
- Optional

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Mandatory

Some properties contain information, such as a printer's name, network address, and configuration information, that is vital to the network.

An object cannot be created without these mandatory values, and the mandatory values cannot be deleted. For example, the name of an object is a required property. (In the user object, the Last Name property is also mandatory.)

Optional

Other properties contain nonvital information, such as a user's title, telephone number, and street address. Objects can be created without this information, and this information can be added or deleted at any time without harming the object.

Many optional properties are multivalued; that is, they can hold more than one value. For example, the user object property Telephone Number can contain several telephone numbers.

eDirectory Object Classes

A *class* is a type of object that serves as a template for a *directory object*. A directory object is defined by a class. This definition is known as an *object class*. For instance, user and organization are object classes.

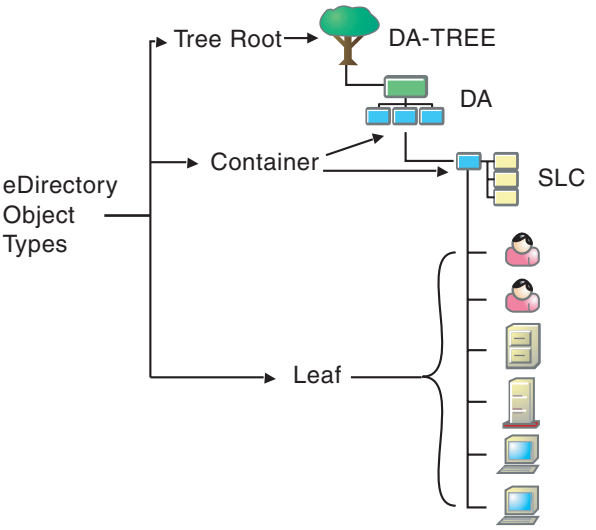
Each class of objects has certain properties. A user object, for example, has Login Name, Password, Last Name, and many other properties.

The schema defines the object classes and properties, along with the rules of containment (which containers can contain which objects).

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

eDirectory object classes can be divided into three categories, as shown in the following figure:

Figure A-6



The three object class categories are

- Tree Object
- Container Objects
- Leaf Objects

Tree Object

The *tree object*, also called *tree root*, is created when you install the first eDirectory server in your network. As the top-most container, it usually holds organization objects, country objects, or alias objects.

The alias object is discussed later in this appendix.

As a network administrator, you can make trustee assignments and grant rights to the entire eDirectory tree from the tree object.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Characteristics of the tree object:

- There is only one per Directory and it forms the top of the eDirectory tree.
- The name of the object is the tree name.
- It can contain only country, organization, security, and alias objects. (The alias object can refer only to objects that can exist in the container the alias object is in; in this instance, the alias object can refer to country and organization objects.)
- It cannot be moved or deleted.

The tree object is sometimes defined as a special type of container because its major function is to contain other objects (it contains the entire Directory).



For more on the eDirectory tree, see the online documentation at www.novell.com/documentation.

Container Objects

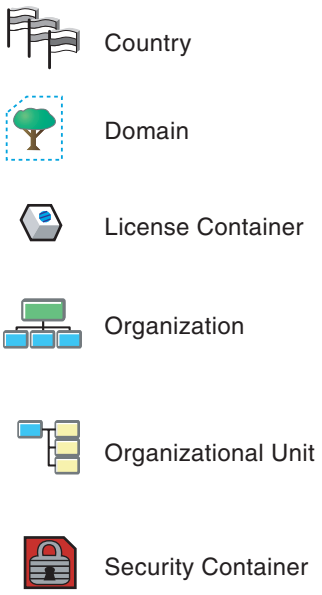
Container objects contain leaf or other container objects. They are used to logically group and organize the objects of your Directory.

They can represent countries, locations within countries, companies, departments, responsibility centers, workgroups, and shared resources.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

The following figure shows the most common classes of container objects:

Figure A-7



The following table lists some of the container objects found in an eDirectory tree:

Table A-1

Container Object	Description
Country (C)	■ Designates the countries where your network resides, and organizes other Directory objects within the country ■ Organizes the eDirectory tree by countries ■ Holds only valid 2-character country abbreviations ■ Optional, but is required for connecting to some X.500 global Directories ■ Exists only in the tree object

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-1**

Container Object	Description
Domain (DC)	■ Helps you further organize other objects in the Directory The domain object exists in the tree object or under organization, organizational unit, and country objects. ■ Represents DNS domain components ■ Allows you to use your DNS location of services resource records (DNS SRV) to locate services in your tree
License Container (LC)	■ Represents a special container object in eDirectory. License container objects can contain one or more license certificate objects. ■ Created when you install a license certificate or create a metering certificate using Novell Licensing Services (NLS). ■ Added by the tree when an NLS-enabled application is installed. A License Certificate leaf object is also added to that container.
Organization (O)	■ Helps you organize other objects in the Directory. The organization object is a level below the country object (if you use the country object). ■ Organizes objects by organizational groups, such as company, university, or department. ■ Exists in the tree or country object. ■ Is required.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-1**

Container Object	Description
Organizational Unit (OU)	■ Helps you further organize other objects in the Directory. The organizational unit object is a level below the organization object. ■ Organizes objects by subunit groups, such as division, business unit, project team, or department. ■ Exists in country, organization, and organizational unit objects. ■ Is optional.
Role-Based Service (RBS)	■ Allows you to specify the tasks that users are authorized to perform in specific administration applications. Defining an RBS role includes creating an RBS role object and specifying the tasks that the role can perform. In some cases, administration applications might provide a few predefined RBS role objects that you can modify.
Security (S)	■ Holds global policies that relate to security properties such as login, authentication, and key management.

The following table lists the distinguishing characteristics of each type of container object:

Table A-2

Container Object	Can Exist In	Can Contain	Example
Country	Tree	Organization	US
		Alias	FR
Organization	Tree	Organizational Unit	Novell
	Country		UCLA
		All leaf objects	

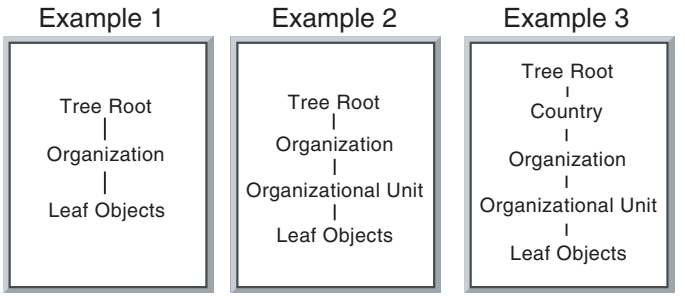
Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-2**

Container Object	Can Exist In	Can Contain	Example
Organizational Unit	Organization Organizational Unit	Organizational Unit All leaf objects	Marketing Sales

The following provide three examples of eDirectory tree structures:

Figure A-8



Container restrictions lead to the following hierarchical tree structure:

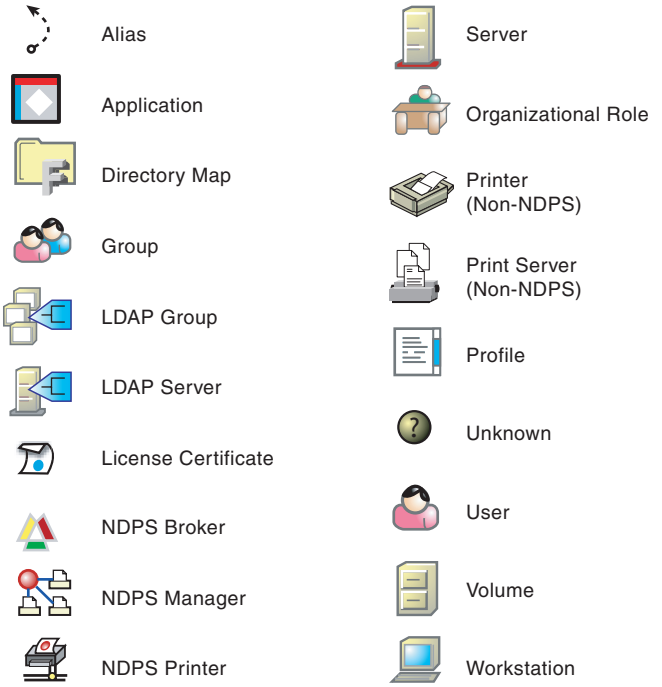
- The tree object must be at the top.
- Country objects are in the tree object.
- Organization objects are in tree or country objects.
- Organizational unit objects are in organization objects or in other organizational unit objects.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Leaf Objects

Leaf objects represent network resources, such as users, workstations, servers, and NetWare volumes. Some of the most common leaf objects are as follows:

Figure A-9



Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

The following table explains the most common eDirectory leaf objects:

Table A-3

Leaf Object	Description
AFP server	Represents an AppleTalk Filing Protocol (AFP) server that operates as a node on your eDirectory network. It usually also acts as a NetWare router to, and the AppleTalk server for, several Macintosh computers.
Alias	Represents another object, which can be a container, user object, or any other object in the tree. An alias object does not carry trustee rights of its own. You can create an alias object that points to another object in the tree. Alias objects give users a local name for an object that lies outside their container.
Application	Represents a network application. Application objects simplify administrative tasks such as assigning rights, customizing login scripts, and launching applications.
Computer	Represents a computer on the network.
Directory map	Refers to a folder in the file system. The directory map object is a pointer to a path in the server file system. It allows you to make simpler references to directories.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-3**

Leaf Object	Description
Group	Assigns a name to a list of user objects in the Directory. You can assign rights to the group instead of to each user; the rights then transfer to each user in the group. Group objects have two main purposes: ■ They allow you to grant rights to a number of user objects at the same time. ■ They allow you to specify login script commands using the IF MEMBER OF syntax.
LDAP group	Represents an LDAP group. The LDAP group object stores configuration data that can be applied to a single LDAP server or to a group of LDAP servers. The LDAP group configures the class and attribute mappings and security policies on the server. This greatly simplifies configuration changes, because one configuration change can be applied instantly to multiple LDAP servers. During installation, an LDAP group object named LDAP Group *server_name* is created in the same container as the server object.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-3**

Leaf Object	Description
LDAP server	Represents an LDAP server. The LDAP server object stores configuration data for an LDAP Services for eDirectory server. During installation, an LDAP server object named LDAP Server *server_name* is created (where *server_name* is the name of the server LDAP Services for eDirectory is installed on). The LDAP server object is created in the same container as the server object. Each LDAP server object configures one LDAP Services for eDirectory server. Do not assign the same LDAP server object to more than one LDAP Services for eDirectory server. If you do, it is no longer assigned to the previous server.
License certificate	Represents a license certificate. Use with NLS to install product license certificates as objects in the database. License certificate objects are added to the Licensed product container when an NLS-aware application is installed.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-3**

Leaf Object	Description
NDPS broker	Represents the NDPS broker. The broker provides three network support services: the Service Registry Service, Event Notification Service, and Resource Management Service. Each eDirectory tree should have at least one NDPS broker. You might want to create additional brokers in certain situations. For example, you might want to create a broker on a local server for each site on a WAN.
NDPS manager	Represents the NDPS manager. An NDPS manager provides a platform for printer agents that reside on the server. An NDPS manager must be created as an object in the eDirectory tree before you can create server-based printer agents. The NDPS manager object stores information used by NDPSM NLM. You can manually load this NLM at the server console. A single NDPS manager can control any number of printer agents. A specific NDPS manager can be loaded on only one server. If it controls a local printer, it must be loaded on the server the local printer is attached to.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-3**

Leaf Object	Description
NDPS printer	Represents the NDPS printer. NDPS printers added to the eDirectory tree by iManager are referred to as *controlled access printers*. As eDirectory objects, NDPS printers are no longer available directly as public access printers. They are available to users only through the eDirectory object list instead of through the list of public access printers.
Organizational role	Defines a position or role within an organization where the users who occupy the position might change, but the position's responsibilities do not change. Users in an organizational role are referred to as *occupants*.
Print queue	Represents a network print queue.
Print server	Represents a network print server.
Printer	Represents a network printing device.
Profile	Represents a login script used by a group of users who need to share common login script commands. The users don't have to be in the same container.
Server	Represents a server running any operating system. A server object is created in the tree when you install eDirectory on a server. The object class can be any server running eDirectory. You can also create a server object to represent a NetWare 2 or NetWare 3 bindery server.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

(continued) **Table A-3**

Leaf Object	Description
Template	Represents standard user object properties that can be applied to new user objects. You can use a template object to facilitate the tasks of creating a user object and setting properties to control login and the user's network computing environment.
User	Represents a person who uses your network. A user object is required for logging in. When you install the first server into a tree, a user object named Admin is created. Log in as Admin the first time.
Unknown	Represents an object for which iManager has no custom icon.
Volume	Represents a physical volume on the network. When you create a physical volume on a server, a volume object is created in the tree. By default, the name of the volume object is the server's name, with an underscore and the physical volume's name appended (for example, DA1_SYS). Volume objects are supported only on NetWare. UNIX file system partitions cannot be managed using volume objects. The volume object in eDirectory does not contain information about the files and directories on that volume. However, you can access that information through iManager. File and folder information is retained in the file system itself.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

eDirectory Object Context and Naming Conventions

To understand the flow and design of an eDirectory tree, you need to know the following:

- What Context Is
- Object Naming Conventions

What Context Is

Context can be defined as

- An Object's Position in the eDirectory Tree

 or

- A Position You Navigate to in the eDirectory Tree After Logging In

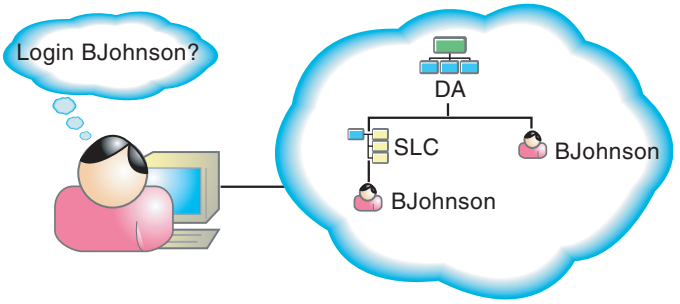
An Object's Position in the eDirectory Tree

When used to define an object's position in the eDirectory tree, the *context* is a list of container objects leading from the object to the tree object. (Locating an object through the context is similar to locating a file using the directory path.)

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

For example, in the following figure, the difference between the two BJohnson user objects is their context. The user object on the left is in SLC container; the user object on the right is in DA container.

Figure A-10



An eDirectory tree cannot have two leaf objects with the same name in the same container. However, an eDirectory tree can have two leaf objects with the same name in different containers because their context is different.

The context for the BJohnson object on the left is BJohnson.SLC.DA; the context for the BJohnson object on the right is BJohnson.DA.

A Position You Navigate to in the eDirectory Tree After Logging In

When you navigate to another location in the eDirectory tree, your context is your current position, or current context, in the tree. It is not where your user object resides in the eDirectory tree.

Current context

- Affects how much of an object's distinguished name (explained later in this section) you must provide with a command to access the resource.
- Identifies the default eDirectory container for your workstation in the Novell client (if you didn't change your context after logging in).

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

- Allows you to refer to an object in your current context by its common name because your current context and the object's context are the same.

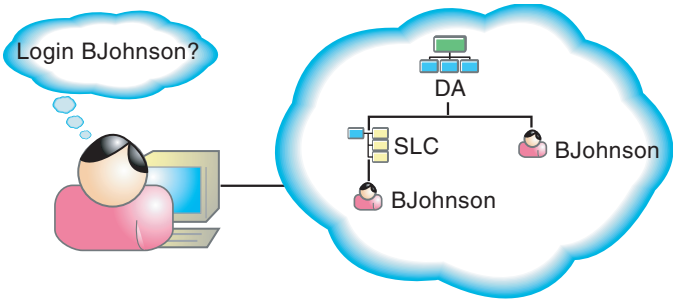
Current context is sometimes referred to as name context.

Object Naming Conventions

Naming conventions allow you to precisely identify and locate objects in your tree.

For example, in the following figure, two user objects named BJohnson exist in separate containers in the Directory. If you log in as BJohnson, which user object would eDirectory use?

Figure A-11



You, or your workstation, must provide eDirectory with enough information to locate the object in the eDirectory tree. You specify this information in the object name.

Each object name exactly identifies an object in the eDirectory tree. So, in the figure above, the exact names are different because their object names contain information that identifies their locations in the eDirectory tree.

To understand object names, you must understand

- Object Name Attributes
- Object Naming Rules

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Object Name Attributes

The name of each object you create in the eDirectory tree consists of the following:

- Name Attribute type
- Name Value

The *attribute type* of the object name determines if the object will be accessed as a container or leaf object in the eDirectory tree.

The *value* of the object is the name you enter for the object when you create it.

The following name attribute types are assigned to the most common eDirectory objects:

Table A-4

Attribute Types	Description	Example
C	Country	C=IR (IRELAND)
O	Organization Name	O=DA
OU	Organizational Unit Name	OU=SLC
CN	Common Name	CN=BJohnson (includes all leaf objects)

Name attribute types

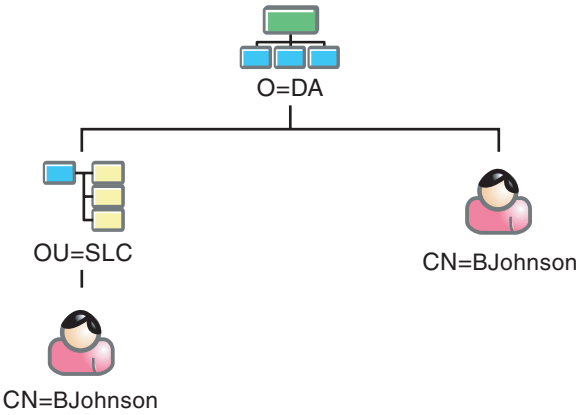
- Distinguish between the different container types and leaf objects.
- Appear before the object they identify.
- Have an equal sign (=) placed between the attribute type abbreviation and the object.
- Are optional (see “Typeless Naming” on A-43), but help to avoid problems that can occur with typeless naming.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A leaf object's common name (CN) is the name shown next to the leaf object in the eDirectory tree.

For example, the common name for both user objects in the following is BJohnson:

Figure A-12



The CN name attribute applies to all leaf objects. Any server, user, group, or other leaf object is named CN=*value*.

When users need to access a resource such as a server in the eDirectory tree, the common name for the server object must be included in the request.

To use a resource outside the user's parent container, the user must change his or her location, or context, in the eDirectory tree.

Object Naming Rules

Before you specify an object by its name, you must understand object naming rules. You can specify the object by using the following:

- Distinguished Name
- Relative Distinguished Name
- Typeful Naming

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

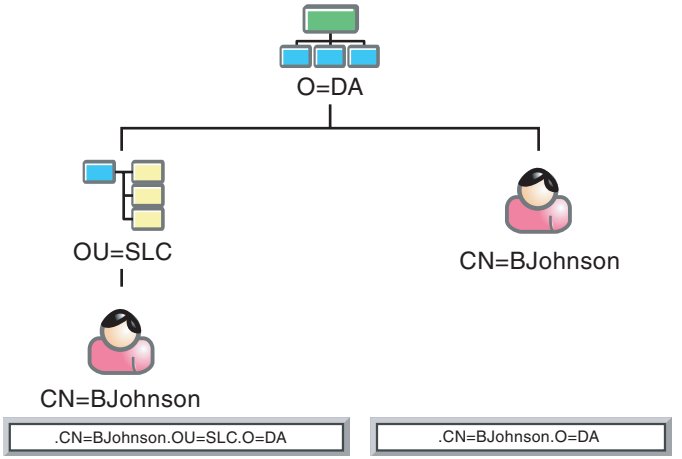
- Typeless Naming

Distinguished Name

An object's *distinguished name* is a combination of its common name and its context. This identifies the object all the way to the top, or root, of the tree. Using Figure A-13 as an example, the distinguished name must include the path up to O=DA.

An object is exactly identified with a distinguished name. Two objects cannot have the same distinguished name.

Figure A-13



In the figure above, the distinguished name for the user object BJohnson in the organizational unit SLC in the organization DA is as follows:

.CN=BJohnson.OU=SLC.O=DA

The distinguished name for the user object BJohnson in the organization DA is as follows:

.CN=BJohnson.O=DA

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

A distinguished name starts with a leading period. The objects in the name are separated by periods, similar to the way names are separated by backslashes in DOS paths.

The names of all objects, from the tree object to the object being named, are included in the distinguished name.

Relative Distinguished Name

A *relative distinguished name*

- Lists the path of objects leading from the object being named to the container representing the object's current context, or current location, in the eDirectory tree.
- Does not start with a leading period.
- Uses periods to separate objects in the name.
- Can use a trailing period.

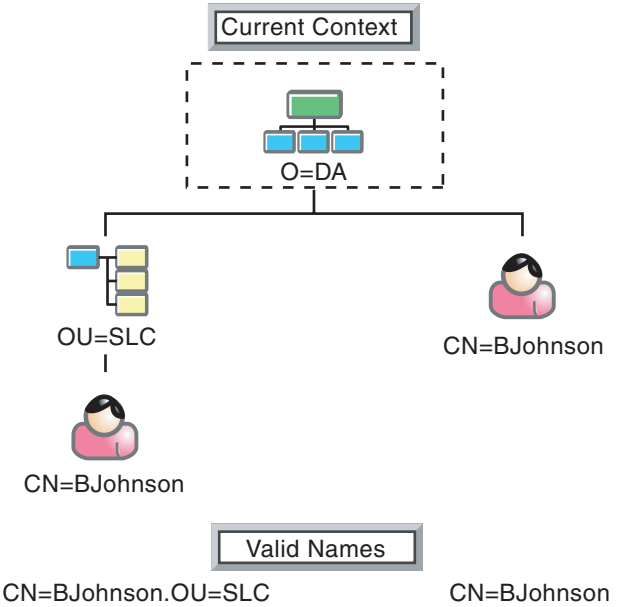


See Novell eDirectory online documentation at http://www.novell.com/documentation/edir873/index.html for more information on trailing periods.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

For example, if your current context is O=DA, you can refer to each BJohnson user object as shown in the following:

Figure A-14



When you use a relative distinguished name, eDirectory must build a distinguished name from it. This is accomplished by appending the relative distinguished name to the current context:

Relative Distinguished Name + Current Context = Distinguished Name

In the following examples, a different current context creates a different distinguished name when the same relative distinguished name is submitted:

Table A-5

Name Submitted	Current Context	Resulting Distinguished Name
CN=BJohnson	O=DA	.CN=BJohnson.O=DA
CN=BJohnson	OU=SLC.O=DA	.CN=BJohnson.OU=SLC.O=DA

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.



A common name (CN) is a relative distinguished name.

A trailing period serves as a shorthand way of changing the current context. Simply put, a trailing period removes the leftmost container from the current context.

For example, the user CN=BJohnson.O=DA is in a situation where the current context on the client machine he is using is OU=SLC.O=DA.

If he simply logs in as CN=BJohnson, the current context will be appended to his name and eDirectory will see him as CN=BJohnson.OU=SLC.O=DA. This is not how he wants to authenticate.

The simplest way for him to log in as the correct user is to put a trailing period at the end of his relative distinguished name, like this:

CN=BJohnson.

The trailing period removes the leftmost container from the current context, which changes the current context from OU=SLC.O=DA to just O=DA. He then gets logged in as CN=BJohnson.O=DA.

Typeful Naming

A *typeful name* uses attribute type abbreviations (such as CN or OU) to distinguish between the different container types and leaf objects in an object's distinguished or relative distinguished name.

Although not mandatory, attribute types help avoid the confusion that can occur with *typeless* naming (explained next).

For example, the following is a typeful name:

.CN=BJohnson.O=DA

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Typeless Naming

A *typeless name* (the most popularly used naming convention) does not include the object attribute type. For example, the typeless distinguished name for .CN=BJohnson.OU=SLC.O=DA is

.BJohnson.SLC.DA

If you do not provide a typeful object name, eDirectory calculates attribute types for each object. The objects cannot be located if the utility places the wrong attribute on the object.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Components of a Solid eDirectory Foundation

To learn about the components of a solid eDirectory foundation, you need to know the following:

- The eDirectory Foundation Model
- eDirectory Network Configuration Recommendations

The eDirectory Foundation Model

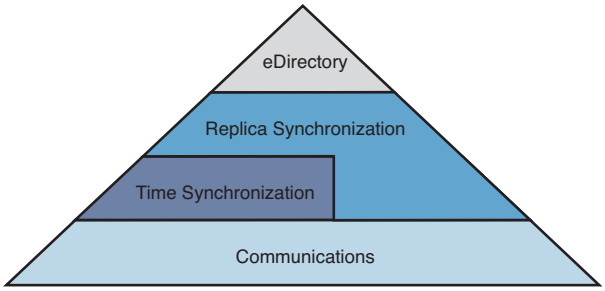
Good design principles are the foundation for a smoothly-running eDirectory system. eDirectory can only perform at its best when the infrastructure where it resides is operating efficiently.

eDirectory relies on a foundation of error-free communications, accurate time synchronization, and efficient replica synchronization.

When the underlying services are designed to operate smoothly, eDirectory operates at its best. When the underlying services are not designed to operate smoothly, the poor performance of these services results in poor eDirectory performance.

The following diagram illustrates the foundation services on which eDirectory relies for smooth operation:

Figure A-15



Time synchronization and replica synchronization depend upon a foundation of solid network communication. Without solid communication, these services cannot function well.

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Replica synchronization operates independently of time synchronization, but it relies on accurate time stamps to make sure that replicas are synchronized properly.

With these foundation services in place and functioning properly, eDirectory is able to function smoothly and efficiently. Without them, eDirectory will not be able to function at its best, and might not function at all.

Once network communications are established on your Linux servers, you can configure your time synchronization, and then eDirectory can be installed.



The eDirectory foundation model might imply that you must establish replica synchronization before you can install eDirectory. As you proceed through the course, you will learn that replica synchronization cannot be configured or monitored until after eDirectory is installed.

eDirectory Network Configuration Recommendations

Linux servers, like Windows servers and workstations, can be configured to receive an IP address, subnet mask, gateway address, and a host and domain name dynamically through DHCP.

However, Novell strongly recommends that eDirectory servers by statically configured. The eDirectory service itself does not require it, but the services that use eDirectory are much easier to maintain if the IP address is static.

Also, it is easier to configure time synchronization if all the servers in the network have static IP addresses.

Network services that use eDirectory also benefit if the host name is statically assigned and mapped to the IP address in the hosts file.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

Index

A

ACL 2-70
address 3-27, 3-37, 3-62, 3-68, 8-45, 8-52–8-53, 8-55, 8-69, 8-141, 9-8
administration A-12
agent 5-68, A-7–A-8
Apache 1-15, 1-21–1-22, 1-45–1-46, 1-54, 1-58–1-59, 1-65, 7-6, 7-10, 7-12, 7-57–7-58, 8-22, 8-37, 8-48, 8-51, 8-73–8-74, 8-89, 8-100, 9-5, 10-15, 10-17, 10-20, 10-23, 10-25, 10-27–10-28, 11-3, 11-8–11-9, 11-27, 11-29
attribute 9-17, 10-24

B

back-end 7-12, 11-17–11-19
background 2-6, 2-26, 2-36, 2-41, 3-12, 3-52, 3-54, 3-61, 3-79–3-80, 8-15, 8-115, 8-119, 8-122, 8-138
backup 1-15, 1-22, 11-3, 11-9
bandwidth 5-33, 8-17, 8-81
binary 3-43, 5-79
BIND 4-3
bindery 2-40, 3-28, A-32
block 6-3, 6-36
bootable 1-37, 1-57, 2-54
broker 7-7, 7-11

C

cache 2-28
Certificate Authority 11-15
CIFS 1-15, 10-22
class 1-6, 1-34–1-37, 1-54, 1-56, 3-82, 9-12, 9-14, A-18, A-20–A-21, A-29, A-32
client 5-51, 6-23, 7-34, 11-18, A-35
cluster 1-17, 1-22, 1-25, 1-62–1-63, 2-16, 3-20, 3-23, 3-89, 5-34, 5-45–5-46, 5-63, 11-4, 11-9, 11-11
clustering 1-6, 1-15, 1-22, 5-54, 11-3, 11-9
commands 2-31, 2-38, 2-79, 8-48
compatibility 1-31, 2-61, 3-20–3-21, 3-67, 3-90, 6-6, 6-15–6-17, 9-4
component Intro-19, 1-1, 1-9, 1-29, 1-34–1-35, 1-43, 1-54, 1-58, 1-65–1-66, 1-69–1-70, 1-72–1-73, 1-77, 2-7, 2-15–2-17, 2-21, 2-83, 3-9, 3-37, 3-39, 3-86, 3-88, 5-62, 5-79, 5-82, 5-85, 6-6–6-7, 6-31, 6-35, 7-5–7-13, 7-57–7-58, 8-11, 8-18, 8-26, 8-30, 8-35–8-37, 8-40, 8-42, 8-146, 9-2, 9-5, 10-20, 10-22, 10-28, 11-17, 11-25, 11-30, A-5–A-6, A-8, A-16, A-24, A-44
compression 3-12, 5-55
concurrent 1-38
configuration 1-14, 1-45, 1-53, 1-60, 1-67, 2-3, 2-15, 2-18, 2-21–2-23, 2-32, 2-39, 2-42–2-43, 2-49, 2-51, 2-56, 2-65, 2-70, 2-72–2-73, 2-81, 2-83, 3-3, 3-7–3-8, 3-10, 3-19, 3-22–3-23, 3-27, 3-29, 3-32–3-34, 3-37, 3-40, 3-49, 3-53–3-56, 3-60, 3-73–3-75, 3-78–3-79, 4-3, 4-6–4-10, 4-13–4-15, 4-17, 5-2, 5-8–5-9, 5-30, 6-4, 6-6, 6-11, 6-18–6-22, 6-31, 6-34, 6-36, 7-7–7-8, 7-10, 7-15–7-18, 7-20, 7-22, 7-24, 7-29, 7-40, 7-46, 7-53–7-54, 7-59, 8-17–8-18, 8-21–8-23, 8-30–8-31,

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

8-35–8-36, 8-42–8-47, 8-49–8-50, 8-54–8-55, 8-68, 8-85, 9-2, 9-4, 9-19, 10-11, 10-17, 10-19, 10-30, 11-2, 11-27, A-20, A-29–A-30, A-45

configure Intro-4, Intro-8, 1-68, 1-74, 2-14, 2-18–2-21, 2-26, 2-42, 2-55, 2-61, 2-73, 3-4, 3-7–3-8, 3-19, 3-23–3-25, 3-33–3-34, 3-40–3-41, 3-48, 3-50, 3-63, 3-72–3-73, 3-75–3-78, 3-81, 3-83–3-84, 3-87, 3-91, 3-100, 3-102–4-4, 4-6, 4-8–4-9, 4-12–4-17, 5-4, 5-8, 5-11–5-14, 5-16, 5-20, 5-30, 5-34, 5-38–5-39, 5-44, 5-60, 5-88, 5-91, 6-1–6-2, 6-18–6-19, 6-27, 6-29, 6-34, 7-9–7-11, 7-13, 7-17, 7-31, 7-35, 7-41–7-42, 7-56, 7-60–7-61, 8-1–8-2, 8-19–8-20, 8-22, 8-30–8-31, 8-33, 8-35–8-38, 8-43, 8-45–8-47, 8-49–8-50, 8-53–8-54, 8-57–8-58, 8-63–8-64, 8-69, 8-77, 8-89–8-90, 8-92–8-93, 8-102–8-104, 8-113, 8-121, 8-135, 8-137, 8-140, 8-147–8-148, 9-1–9-2, 9-6–9-8, 9-12, 9-16–9-17, 9-19, 9-23–9-25, 10-10, 10-18–10-19, 10-34, A-45

ConsoleOne 5-50

container 10-13, A-24

context 3-28, A-41

core dum 1-37, 1-57

create Intro-10, 1-26, 1-32–1-33, 1-40, 1-42, 1-59, 1-62, 1-64, 2-41, 2-44, 2-60, 2-69, 2-72, 3-2, 3-20, 3-35, 3-58, 3-72, 3-75, 3-80–3-82, 3-91, 3-93, 4-8–4-9, 4-15, 5-18, 5-29, 5-34, 5-40, 5-45, 5-47–5-49, 5-52–5-56, 5-59, 5-68, 5-70–5-75, 6-11, 6-23, 6-32–6-35, 7-7–7-8, 7-10–7-11, 7-13, 7-15–7-16, 7-18–7-20, 7-22–7-24, 7-26, 7-29, 7-35, 7-41, 7-46, 7-49, 7-51, 7-58–7-59, 8-12, 8-14, 8-27, 8-35, 8-37, 8-44–8-45, 8-48, 8-72–8-73, 8-76, 8-102–8-103, 8-111–8-113, 8-115, 8-119–8-120, 8-123, 8-125–8-129, 8-135, 8-142–8-143, 9-2, 10-13–10-14, 10-16, 10-19–10-24, 10-27, 10-30, 10-36, 11-13, 11-15–11-16, 11-24, A-19, A-24, A-28, A-31–A-33, A-37

cursor Intro-12–Intro-13, 2-10

D

database A-3, A-6–A-7

deactivate 5-54–5-55

Deployment Manager 1-33, 11-16

device 5-54, 5-56, 8-130

DHCP Intro-1, Intro-4–Intro-5, Intro-8, 1-16, 1-21, 1-23, 1-45, 1-58, 2-21, 4-1–4-4, 4-13–4-17, 11-3, 11-8–11-9, 11-27, A-45

diagnose 2-40, 2-48, 3-24–3-25, 3-32, 3-34, 3-64

DIB A-9

directory Intro-13, 1-2, 1-5, 1-8, 1-10–1-12, 1-14, 1-27, 1-29–1-30, 1-45, 1-50–1-53, 1-57, 1-59, 1-63–1-64, 1-73–1-74, 2-11–2-13, 2-17, 2-21–2-22, 2-35–2-36, 2-38, 2-43–2-44, 2-54, 2-59, 2-62, 2-64–2-77, 2-79–2-82, 3-4, 3-6, 3-9, 3-11, 3-14, 3-17, 3-22, 3-26, 3-33, 3-35–3-36, 3-48, 3-50–3-51, 3-54–3-55, 3-59–3-60, 3-67, 3-80, 3-86–3-87, 3-89, 4-3–4-4, 4-9–4-11, 4-13, 5-17, 5-20, 5-23, 5-32, 5-36, 5-40, 5-42, 5-44, 5-46–5-47, 5-50–5-52, 5-58–5-60, 5-63, 5-65–5-67, 5-69, 5-74–5-75, 5-77, 5-86, 6-4, 6-6, 6-8, 6-10, 6-12, 6-16–6-17, 6-19, 6-28, 6-31, 6-33, 7-15, 7-34–7-35, 7-42, 7-55, 8-6, 8-8–8-9, 8-13, 8-15–8-16, 8-19–8-20, 8-22–8-24, 8-28, 8-35–8-37, 8-40, 8-42, 8-44–8-45, 8-47, 8-57, 8-61–8-62, 8-64–8-65, 8-69, 8-71–8-72, 8-74–8-76, 8-86, 8-111, 8-125–8-126, 8-128–8-130, 8-140, 8-142, 9-2, 9-4, 9-6, 9-10–9-13, 9-17–9-18, 10-2, 10-5, 10-12–10-13, 10-15, 10-17–10-22, 10-25–10-29, 10-31–10-32, 10-36–10-37, 11-2, 11-11–11-16,

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

11-19–11-21, 11-23, 11-25, 11-27–11-28, A-2–A-11, A-13–A-14, A-16–A-17, A-20, A-22–A-25, A-28–A-29, A-34, A-36
DirXML 3-60, 6-11, A-15
disk space 1-70
distinguished name 3-39, 6-31, A-35, A-41
DNS Intro-1, Intro-4–Intro-5, Intro-8, 1-16, 1-21, 1-23, 1-45, 1-58, 2-21, 2-23, 2-48, 3-27–3-28, 3-37, 3-51–3-52, 3-63, 3-70, 3-94, 4-1–4-12, 4-14, 4-16–4-17, 5-27, 5-68, 5-72, 6-32, 7-15–7-18, 7-34, 7-39–7-41, 7-47, 7-52, 7-54–7-56, 7-58, 7-62, 8-21, 8-24–8-25, 8-52–8-53, 8-55–8-58, 8-61–8-62, 8-68–8-69, 8-84, 8-87–8-88, 8-90, 8-114, 8-118, 8-120, 8-141, 10-14–10-15, 10-18, 10-20, 10-23, 10-25, 10-27, 11-3, 11-8–11-9, 11-27, A-24
Domain
 Name Service 4-4
domain 1-31, 10-13, 10-30, 10-32, A-24
driver 7-14

E

eDirectory Intro-6, 3-59, 7-52, 9-6–9-7
encrypted 2-47, 5-24, 5-45, 5-55–5-56, 6-7–6-8, 6-32, 7-5, 8-11, 8-22–8-23, 9-20, 10-12, 11-17
encryption 7-4
export 2-41, 2-55
external 2-39, 3-36, 5-6–5-7, 5-33, 7-42

F

FAT 1-57
FCS 1-56
file
 access 6-10, 10-18, 10-20, 10-23
 system 1-18, 1-25–1-28, 1-52, 2-2, 2-10–2-12, 2-35–2-36, 2-43–2-44, 2-61–2-66, 2-68–2-71, 2-73, 2-82, 2-85, 3-2, 3-35–3-36, 3-43, 3-45, 5-25, 5-31–5-32, 5-35–5-37, 5-39, 5-41, 5-44–5-45, 5-47, 5-50–5-52, 5-57, 5-59–5-60, 5-64–5-65, 5-67, 5-73, 6-1–6-4, 6-7–6-8, 6-26–6-27, 6-29, 8-23, 8-27–8-28, 8-33, 8-75, 8-82, 8-86, 8-129–8-130, 10-14, 10-21–10-22, 10-26–10-27, 11-6, 11-11–11-14, 11-19, A-28, A-33
frame 3-56–3-57

G

generate 1-62, 3-35
global Intro-7, 4-9, 4-14, 5-26, 6-11, 6-31, A-4–A-5, A-10, A-23, A-25
graphical
 user interface 2-24
group 2-78, 3-93, A-29
GUI 1-66, 1-71, 2-15, 2-18–2-19, 2-23, 2-45, 2-50, 2-79
GUID 8-21, 8-24, 8-61, 8-88

H

hardware Intro-3, Intro-20, 1-5–1-8, 1-34–1-36, 1-54, 1-56, 2-3, 2-18, 2-23, 2-39–2-40, 2-66, 2-69, 3-2, 3-19, 3-23, 3-33, 5-56, 7-14, 8-17–8-18, 8-35, 8-65, 11-22–11-23, A-10
header 3-29, 3-31, 3-54, 3-79–3-80, 8-141
health 1-16, 1-23, 1-67, 2-40, 3-2–3-4, 3-19–3-25, 3-31–3-34, 3-48, 3-51, 3-54, 3-58, 3-60, 3-64, 3-86–3-99, 3-102, 7-7, 8-74, 11-4
 check 1-67
hexadecimal 3-80, A-14
high availability 2-62

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

HTTP 8-50–8-51
HTTPS 3-69, 8-51

I

identity 3-12
iFolder Intro-1, Intro-4, Intro-8, Intro-20, 1-6, 1-17, 1-19, 1-23, 1-33, 1-35–1-36, 1-46, 1-57, 1-59, 2-16, 3-37, 5-25, 5-59–5-60, 8-1–8-58, 8-60–8-81, 8-83–8-93, 8-96–8-98, 8-100, 8-102–8-109, 8-111–8-149, 10-2, 10-5, 10-8, 10-10, 10-12–10-13, 10-15, 10-19–10-20, 11-4, 11-10, 11-17–11-20, 11-22, 11-28, 11-30, A-17
iManager Intro-4–Intro-5, Intro-19, 1-7, 1-38, 1-44, 1-46, 1-49, 1-52–1-53, 1-55, 1-58, 1-70, 2-23, 2-37, 2-42, 2-53, 3-1–3-2, 3-4, 3-31, 3-39, 3-67–3-73, 3-75–3-81, 3-83–3-86, 3-88–3-92, 3-102, 4-3–4-4, 5-26–5-29, 5-45, 5-50–5-51, 5-53–5-54, 5-57, 5-66, 6-13, 6-16–6-17, 6-19, 6-21–6-26, 6-34, 7-6, 7-10, 7-13–7-15, 7-18–7-22, 7-24, 7-26–7-30, 7-55, 7-57, 7-59, 8-6, 8-9, 8-12, 8-19–8-20, 8-31, 8-35–8-36, 8-38–8-39, 8-44, 8-47, 8-51–8-58, 8-60–8-63, 8-75–8-77, 8-79, 8-83, 8-85, 8-87, 8-92, 8-101–8-104, 8-109, 8-146, 8-148, 10-11, 10-17–10-18, 10-20, 10-23, 10-25, 10-27, 10-32–10-33, 10-36, 11-26, 11-28, A-19, A-32–A-33
installation 5-53, 7-13, 7-58, 10-32
Internet Printing Protocol 7-4
interval 3-97, 5-46, 8-62, 8-79, 8-82–8-83, 8-88–8-90, 8-97–8-98, 8-101, 8-108, 8-122–8-124, 8-137–8-138
intranet 7-37
IP
 address 8-52–8-53, 8-55, 8-69, 8-141
IPP 3-20, 3-23, 7-4–7-5, 7-7, 7-34, 7-39–7-41
iPrint 7-13–7-14, 7-18–7-19, 7-21–7-22, 7-24, 7-26–7-30, 7-43–7-44, 7-55
IPX 1-16, 1-24, 11-4, 11-10

J

JReport 1-67

L

LAN 2-38–2-39, 2-57, 3-19, 3-23, 3-98, 5-33
LDIF 2-41
limit 8-81–8-82
Linux 1-22, 1-24–1-25, 2-17, 2-21, 3-6, 3-17, 3-19, 3-33, 3-36, 3-50, 5-21, 5-31, 5-66, 8-34, 8-36, 9-11, 10-2, 10-12, 10-18, 10-31–10-32, 11-21–11-22, 11-24, A-12
LOAD Intro-17, 1-57, 1-63, 1-66, 2-41, 2-43, 2-57, 3-25, 3-28, 3-62, 3-97, 5-57, 5-68, 6-13, 7-17, 7-20–7-21, 7-30, 9-20, A-31
location 3-52, 3-92
location-based 7-4–7-5, 7-41–7-42
log 2-24
logical 2-52, 5-35, 5-47–5-48, A-2, A-4–A-5, A-11, A-16
login
 script 10-14

M

manage 8-56
management Intro-19–Intro-21, 1-3, 1-7, 1-10–1-13, 1-18, 1-26–1-27, 1-38, 1-44, 1-46, 1-51, 1-57–1-59, 2-7, 2-14, 2-17–2-18, 2-21, 2-37, 2-56, 2-60, 2-81–2-82, 3-3–3-4, 3-20, 3-22, 3-26, 3-28, 3-38, 3-67–3-68, 3-83, 3-86, 3-88, 3-96, 4-3–4-4, 4-14, 5-2, 5-20–5-21, 5-27–5-30, 5-35, 5-45, 5-50–5-52, 5-54–5-56, 5-62–5-63, 5-65–5-66, 5-68, 5-90, 6-5–6-7, 6-11, 6-13, 6-15–6-17,

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

6-21, 6-26, 6-34, 6-36, 7-7, 7-10, 7-28, 7-32, 7-47, 7-53, 7-61, 8-6, 8-15, 8-21, 8-29, 8-35, 8-37, 8-56–8-57, 8-61, 8-63, 8-88, 8-101, 8-111, 8-145, 8-147, 8-149, 11-5, 11-8, 11-13, 11-26, 11-28, A-2, A-4, A-10–A-13, A-15, A-25, A-31

map 2-44, A-28

master 2-7, 4-9, A-8

media 2-68–2-69

memory Intro-12, 1-34–1-35, 1-37, 1-56, 2-39, 2-45, 2-62, 3-3, 3-19–3-20, 3-23, 3-25, 3-31–3-33, 3-43, 3-47, 3-88, 3-94, 3-97, 5-46, 8-5

Microsoft

- Microsoft Web Folders 10-5, 10-35

migrate Intro-3–Intro-4, Intro-8, 1-7–1-9, 1-62, 1-64, 2-41, 3-75, 5-1, 5-62, 5-69, 5-72, 5-74, 5-86, 5-88, 7-1–7-2, 7-46, 7-48, 7-56, 7-62

migrating Intro-1, Intro-20, 1-2, 1-31, 1-51, 5-2, 5-45, 5-64, 5-86, 7-46–7-47, 7-54, 7-61–7-62, 8-23

migration 5-2

modify 8-130

monitor 1-49, 2-8, 2-42, 2-45, 2-48, 2-56, 3-2–3-3, 3-19–3-24, 3-32–3-34, 3-50–3-52, 3-54, 3-56, 3-58–3-61, 3-64, 3-86, 3-88, 3-90–3-93, 3-98, 3-102, 7-7

mount

- point 2-68–2-69, 2-71, 5-40–5-41, 5-55, 5-59, 8-46, 8-129–8-130, 10-12

N

name

- space 5-55

Native File Access Pack 6-18

navigation 2-11–2-13, 2-19, 3-24, 3-29, 3-34, 3-36, 3-41, 3-56–3-57, 3-72, 3-80

Navigator 2-11, 8-141, 10-6, 10-35

NDPS 7-10, 7-57

- NDPS Manager A-31

NDS 1-30–1-31, 1-56, 1-59, 1-62, 1-73, 2-42, 3-31, 3-59–3-63, 5-18–5-19, 5-55, 6-5–6-7, 6-9–6-10, 6-15–6-17, 9-6, A-11, A-14

NDSIMONITOR 3-62

NDSPKI 1-60

Netscape 3-61, 9-6, 10-6, 10-35

NetStorage 5-50, 10-15, 10-30

NetWare 1-22, 1-24–1-25, 1-50–1-51, 1-59, 1-63–1-64, 1-74, 1-76, 3-9, 3-11, 4-4, 10-2, 10-8, 10-32, 11-9, 11-12, 11-21, 11-23–11-24

- NetWare FTP Server 1-23, 11-10

network 1-61, 5-14, 5-33, 10-5

- resources 1-12

NFAP 1-15–1-16, 3-28–3-29, 6-9–6-10, 6-18, 11-17

NFS 1-16, 2-66, 5-64, 6-18

NICI 1-16, 1-24, 11-4, 11-11

NLM 1-18, 1-31, 1-66, 2-27, 3-9–3-10, 3-19, 3-21, 3-27–3-30, 3-64, 5-68, 5-85, 6-6, 6-13, 6-18, 7-11, A-31

NMAS 1-16, 1-24, 1-26, 1-72–1-74, 6-6, 6-10–6-14, 6-16–6-17, 11-4, 11-11–11-12

node 2-39, 2-49, 2-67, A-28

Notes 2-38, 3-90, 11-19–11-20

Novell

- Novell Cluster Services 1-17, 1-22, 1-25, 2-16, 3-20, 3-23, 5-45, 11-4, 11-11
- Novell Distributed Print Services 7-10, 7-57
- Novell International Cryptographic Infrastructure 3-9
- Novell Modular Authentication Service 1-72–1-73
- Novell Storage Services Intro-4, 1-21, 1-46, 1-57, 2-16, 2-51, 5-31–5-32, 5-44, 5-53, 5-62, 5-91, 11-8, 11-28

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

NSS Intro-4, Intro-8, 1-6–1-7, 1-17–1-18, 1-21–1-22, 1-25–1-27, 1-46, 1-57, 1-66, 1-74, 2-16, 2-47–2-48, 2-51–2-52, 2-57–2-58, 2-81, 3-25, 5-1–5-3, 5-25–5-26, 5-31–5-36, 5-39, 5-44–5-57, 5-59–5-66, 5-86, 5-88, 5-91–5-92, 6-3–6-4, 6-18–6-19, 6-25, 8-33, 8-35–8-36, 8-43–8-44, 10-10, 10-12, 10-22, 10-25–10-29, 10-37, 11-5, 11-8–11-9, 11-11–11-12, 11-18, 11-28
 volume 5-48

O

object 1-11, 6-15, 7-57, 10-13, A-22, A-24
operating system A-3
options 1-37, 1-56, 5-33, 7-37

P

partition 2-54, 2-67, 2-70
password 2-18, 6-14, 6-35, 8-87
physical Intro-10, 2-54, 2-67, 3-36, 3-43, 3-97, 5-35, 5-47, 5-49, 5-54, 5-56, 5-65, 6-9, 7-7, 7-14, 8-35, A-2, A-6, A-11, A-17, A-33
ping 3-51
PKI 1-17, 1-25, 11-5, 11-12
pool 5-48, 5-54
port 1-15–1-18, 2-21, 3-10, 3-12–3-15, 3-27, 3-29, 3-48, 3-51–3-52, 3-62–3-63, 3-70, 3-95, 5-5, 5-16–5-19, 6-32, 7-10, 7-12, 7-58, 8-50, 8-56, 8-85, 9-10, 10-15–10-16, 10-25, 10-28, 11-3–11-6
post-installation 1-74, 2-21, 5-53
post-migration 7-56
pre-migration 1-45, 1-58, 11-27
print
 data encryption 7-4
 job 7-7, 7-9, 7-12, 7-28–7-29, 7-42–7-44, 7-61, 11-21, A-14
printer Intro-4, 5-72–5-73, 5-86, 7-3–7-11, 7-14–7-19, 7-22–7-29, 7-31–7-35, 7-39–7-41, 7-43–7-44, 7-46–7-48, 7-52–7-54, 7-56–7-62, A-18–A-20, A-31–A-32
 agent 5-73, 5-86, 7-6, 7-24, 7-46–7-48, 7-52–7-53, 7-59, 7-61–7-62, A-31
processor 1-34–1-37, 1-56, 2-55, 3-2, 3-19, 3-23, 3-33, 8-18
project 5-70–5-71, 5-76, 7-53
property 2-79, 3-83, 5-39, 5-55, 5-75–5-76, 6-11, 6-19, 8-112, 8-131–8-133, 8-135–8-136, 10-13–10-14, 10-25–10-28, A-16, A-18–A-20, A-25, A-33
protocol 1-8, 1-13, 1-24, 1-38, 1-45, 2-49, 2-73, 3-2, 3-6, 3-12, 4-3, 5-4–5-5, 5-32–5-33, 5-37–5-38, 5-64, 5-89, 5-91, 6-2, 6-9–6-10, 6-15, 6-18–6-19, 7-4, 8-37, 10-22, 10-24, 11-10, 11-17, 11-19–11-20, 11-27, A-8–A-9, A-28
public
 key infrastructure 1-17, 1-25, 11-5, 11-12
purge 1-26, 3-25, 5-50, 10-28–10-29, 10-37, 11-13

Q

quota 8-80, 8-96, 8-100

R

RAID 1-27, 5-46, 5-54, 5-56, 8-35
read 2-73, 2-80
reliability 2-63
Remote Manager 2-37, 2-45, 3-2–3-3, 3-17, 3-100, 5-25, 5-50, 6-26
rename 7-20
replica
 ring 6-12

 Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

synchronization A-44–A-45
reports 6-13
requirements 1-56
resource 1-12, 1-19, 1-26, 2-7, 5-8, 5-64, 7-47, 7-53, 7-61, 10-14, 10-19, 11-13, A-2, A-11, A-15, A-17–A-18, A-24, A-31, A-35, A-38
management 1-26, 11-13
Resource Management Service 7-47, 7-53, 7-61, A-31
restrictions 1-38
rights 3-73, 3-75, 5-58–5-60
RMS 7-47
role A-32
root 2-29, 2-64, 7-15, 8-46

S

SCSI 2-53, 2-67, 5-33
search
engine 1-19
form 9-17
secondary Intro-5, 3-41, A-9
security 1-3, 1-8, 1-20, 1-29, 1-38, 1-59–1-60, 2-6, 2-23, 3-6, 3-12, 3-29, 4-4, 5-35, 6-7–6-9, 6-11, 6-32, 7-32–7-33, 7-55, 8-4, 8-16, 8-37, 8-57, 8-141, 8-145, 8-147, 9-6, 9-19, 9-25, 10-12, 11-7, 11-15, 11-17–11-19, A-2, A-4–A-5, A-10, A-12, A-15, A-22, A-25, A-29
segments 5-56
server Intro-1–Intro-8, Intro-17–Intro-20, 1-1–1-6, 1-8, 1-10, 1-15–1-17, 1-19–1-27, 1-30–1-38, 1-41, 1-43–1-47, 1-49, 1-51–1-69, 1-72, 1-75–1-76, 2-1–2-4, 2-6, 2-14–2-17, 2-19–2-21, 2-23–2-25, 2-35–2-36, 2-38–2-46, 2-48–2-50, 2-52–2-54, 2-56, 2-58, 2-60, 2-62, 2-68, 2-81–2-82, 2-84, 3-2–3-3, 3-5–3-13, 3-16–3-34, 3-37–3-41, 3-43–3-44, 3-48, 3-51–3-52, 3-54–3-64, 3-66–3-70, 3-75–3-76, 3-78, 3-85–3-90, 3-92–4-1, 4-3–4-6, 4-8–4-14, 4-16–4-17, 5-1–5-31, 5-33–5-34, 5-37–5-41, 5-44, 5-46, 5-48, 5-50–5-51, 5-53–5-55, 5-57, 5-60–5-72, 5-74, 5-77–5-80, 5-82–5-84, 5-86–5-89, 5-91–6-5, 6-8–6-13, 6-15–6-21, 6-29–7-2, 7-5–7-7, 7-10–7-14, 7-16–7-17, 7-19–7-20, 7-27, 7-29, 7-32–7-35, 7-39–7-43, 7-46–7-50, 7-52–7-59, 7-61–8-2, 8-4–8-17, 8-21–8-25, 8-28–8-31, 8-33–8-38, 8-40–8-53, 8-55–8-57, 8-60, 8-62–8-64, 8-66–8-70, 8-74–8-75, 8-83–8-92, 8-95, 8-97–8-98, 8-100, 8-105–8-106, 8-108, 8-113–8-115, 8-118–8-121, 8-124, 8-129, 8-132, 8-136–8-137, 8-139–8-141, 8-143–8-148, 9-1–9-3, 9-5, 9-7–9-8, 9-10, 9-23, 9-25, 10-2, 10-5–10-13, 10-15–10-23, 10-25, 10-27–10-30, 10-32, 10-34–10-36, 11-1, 11-3–11-4, 11-8–11-13, 11-15–11-19, 11-21–11-22, 11-24–11-30, A-1, A-7–A-8, A-14, A-17, A-21, A-28–A-33, A-38
management Intro-19, 2-14, 3-3, 3-22
service 1-72, 5-44, 7-47, A-25
Service Location Protocol 1-27, 3-30
session 2-26
settings 7-35, 7-43–7-44, 10-19
size 8-78, 8-107
SLES 2-17
SLP 1-18, 1-27, 1-31, 3-30, 5-17–5-19, 11-5, 11-13
SMDR 5-68, 5-85
SMS 1-15, 1-18, 1-22, 1-27, 5-61–5-63, 5-68, 5-84, 6-15, 11-3, 11-5, 11-9, 11-13
SNMP 2-56, 4-4, 7-7–7-8, 7-27
software Intro-3–Intro-4, Intro-10, Intro-16, 1-2, 1-5–1-8, 1-18, 1-27, 1-34, 1-40, 1-42–1-43, 1-46, 1-49, 1-55, 1-58, 1-63, 1-66, 1-74, 2-16–2-21, 2-23, 3-9, 3-37, 3-68, 3-94, 4-13, 4-17,

Copying all or part of this manual, or distributing such copies, is strictly prohibited.
To report suspected copying, please call 1-800-PIRATES.

5-32–5-34, 5-37, 5-45–5-46, 5-48, 5-54, 5-56, 5-62, 5-67–5-69, 5-90, 6-5, 6-9, 6-14–6-15, 7-6, 7-11–7-14, 7-31, 7-35–7-38, 7-40–7-41, 7-56, 7-58, 7-60, 8-15, 8-28, 8-35–8-36, 8-39–8-40, 8-67, 8-70, 8-73, 8-90, 11-5, 11-22–11-23, 11-25, 11-28

space 1-70, 5-55, 8-96, 8-100

SSL 3-9–3-10, 3-28, 3-38, 3-61, 3-63, 3-91, 5-16–5-19, 6-31–6-33, 7-4, 7-10, 7-12, 7-58, 8-4, 8-8–8-9, 8-11, 8-15, 8-37, 8-51, 8-68, 8-85, 8-146, 10-12

standalone 4-3

start Intro-6, Intro-10–Intro-12, Intro-14–Intro-15, Intro-17–Intro-18, 1-39, 1-47, 1-63, 1-65, 2-7, 2-10, 2-18–2-19, 2-21, 2-25, 2-27, 2-29, 2-45, 2-67, 2-79, 3-2, 3-32, 3-39, 3-68, 3-71, 3-73, 4-6, 4-11–4-12, 4-16, 5-9, 5-12–5-13, 5-15, 5-57, 5-68, 5-70, 5-86, 6-13–6-14, 6-30, 7-14, 7-16, 7-18–7-20, 7-24, 7-29–7-30, 7-43–7-44, 7-48, 7-53, 7-55, 8-48, 8-53–8-54, 8-63, 8-69, 8-72–8-73, 8-89, 8-91, 8-111–8-113, 8-117, 8-122, 8-148, 10-15, 10-17–10-18, 10-20, 10-23, 10-25, 10-27, 11-16, 11-24, A-40

storage Intro-4, 1-3, 1-13, 1-17–1-18, 1-21, 1-24–1-25, 1-27, 1-45–1-46, 1-57–1-59, 2-16, 2-43, 2-47–2-48, 2-51, 2-53, 2-57–2-58, 2-67, 2-73, 5-2, 5-25, 5-31–5-36, 5-44–5-49, 5-52–5-54, 5-62–5-63, 5-68, 5-91, 6-11, 6-15, 8-2, 8-5, 8-10, 8-17, 8-35, 8-40, 8-63, 8-136, 8-146, 10-2, 10-4–10-5, 10-7–10-10, 10-13–10-14, 10-19–10-31, 10-36, 11-5, 11-8, 11-10–11-11, 11-13, 11-17–11-20, 11-27–11-28, A-2

 area network 5-33

Storage Management Services 1-18, 1-27, 5-62–5-63, 6-15, 11-5, 11-13

structure A-16

subcontainer 1-59–1-60, 6-14

subnet 1-35–1-36, 4-14–4-15, A-45

subsystem 5-32, 5-44

Support Pack 1-3, 1-47, 1-52, 1-55–1-56, 3-24, 3-31–3-32, 3-34, 3-61, 5-62, 5-92, 8-34, 9-5

synchronization 8-124, 11-17

SYS 1-36–1-37, 1-57, 2-70, 3-9–3-10, 3-14, 3-54–3-55, 3-80, 5-40–5-41, 5-48, 5-68, 6-13, 6-29, 7-33, 7-47, A-33

system Intro-4–Intro-5, Intro-10, Intro-17, 1-6, 1-18, 1-20, 1-23, 1-25–1-28, 1-34–1-37, 1-44–1-46, 1-52, 1-55–1-56, 1-63, 1-65–1-66, 1-70–1-71, 2-2–2-3, 2-5–2-7, 2-9–2-12, 2-14, 2-18–2-19, 2-21, 2-23–2-24, 2-26–2-28, 2-31–2-33, 2-35–2-36, 2-43–2-45, 2-47, 2-51, 2-53–2-55, 2-58, 2-60–2-73, 2-76, 2-82, 2-85, 3-2–3-3, 3-9–3-10, 3-19–3-21, 3-23, 3-26, 3-29, 3-35–3-37, 3-42–3-43, 3-45, 3-61, 3-75, 3-83, 3-86–3-88, 3-93–3-94, 3-97–3-98, 3-101, 4-13, 5-4, 5-10, 5-20–5-22, 5-25–5-26, 5-31–5-33, 5-35–5-37, 5-39–5-41, 5-44–5-48, 5-50–5-55, 5-57, 5-59–5-60, 5-62, 5-64–5-65, 5-67–5-69, 5-73, 5-85, 5-90, 6-1–6-5, 6-7–6-9, 6-13, 6-15–6-16, 6-26–6-27, 6-29, 7-8, 7-10, 7-12–7-15, 7-17–7-18, 7-26–7-27, 7-32–7-33, 7-36, 7-44–7-48, 7-54, 7-60–7-62, 8-4, 8-6, 8-9, 8-12, 8-14, 8-16–8-18, 8-22–8-23, 8-25, 8-27–8-36, 8-39–8-40, 8-42–8-47, 8-49, 8-55–8-58, 8-61, 8-65–8-66, 8-68, 8-71, 8-73–8-75, 8-77–8-83, 8-85–8-86, 8-88–8-89, 8-93, 8-96–8-98, 8-100–8-101, 8-104, 8-107–8-108, 8-113, 8-119–8-120, 8-124, 8-129–8-130, 8-138, 8-141, 8-148, 9-5–9-6, 9-24, 10-6, 10-14, 10-21–10-22, 10-24, 10-26–10-27, 10-35, 11-6–11-7, 11-11–11-14, 11-19, 11-26–11-28, A-3–A-4, A-8–A-9, A-12–A-14, A-28, A-32–A-33, A-44

 Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

T

target
server Intro-20, 8-56–8-57
Target Service Agent 5-68
TID 6-11, 6-13, 6-16
time Intro-4, Intro-16–Intro-17, 1-32–1-33, 1-38, 1-44–1-46, 1-54, 1-66, 2-8–2-9, 2-15, 2-23–2-24, 2-28, 2-30, 2-32, 2-36, 2-39, 2-46, 2-54, 2-56, 2-59–2-60, 3-24–3-26, 3-36, 3-75, 3-89, 3-91–3-92, 3-97–3-98, 4-4, 4-10, 4-14–4-15, 5-2, 5-4–5-15, 5-30, 5-46, 5-54–5-55, 5-61, 5-68, 5-83, 5-89, 6-32, 7-11, 7-20, 7-24–7-25, 7-29, 7-35, 7-41, 7-43, 7-54, 7-59, 8-2, 8-8, 8-12, 8-15, 8-22, 8-28, 8-43, 8-45, 8-56, 8-74–8-75, 8-77, 8-79, 8-87–8-88, 8-90–8-92, 8-94, 8-99, 8-113, 8-115, 8-117, 8-119, 8-123, 8-136, 9-3, 9-20, 9-24, 10-2, 10-6, 10-16, 10-19, 10-22, 10-31, 11-15–11-16, 11-26–11-28, 11-30, A-1, A-7, A-16, A-20, A-29, A-33, A-44–A-45
server 5-11–5-12
traditional
volume 2-59, 5-33, 5-35, 10-8, 10-10, 11-18
transaction 4-4, 5-37, 5-46
Transaction Tracking System 5-46
tree 1-59, 5-18–5-19, 11-16, A-7, A-16
TTS 5-46
type 2-71, 3-52, 5-16, 5-82, 6-13, 7-16

U

unattended 1-54–1-55
upgrade Intro-2, Intro-8, Intro-20, 1-1–1-5, 1-9, 1-31–1-32, 1-39, 1-47, 1-49, 1-51–1-56, 1-59–1-69, 1-75–1-76, 1-78, 2-17, 3-31–3-32, 5-34, 6-12, 6-15, 8-34, 8-39, 8-67
upload 3-19, 3-23, 3-28, 3-33, 7-9, 7-15, 7-33, 8-7, 8-76–8-77, 8-90, 8-142–8-143, 10-16
user 6-23–6-24, 8-40, 8-42, 8-58, 8-61, 8-72, 8-93
account 2-23, 6-31, 8-17–8-18, 8-23, 8-25, 8-27, 8-45, 8-79, 8-85, 8-93–8-94, 8-100–8-101, 8-105, 8-113, 8-147
Agent A-7–A-8
interface 2-24
management 3-38, 5-2, 5-21, 5-28–5-29, 5-62, 6-21
name 2-4
object 6-15
utilities 5-50

V

VERIFY 2-57
version 1-31, 8-63
view 5-87
volume 3-26, 5-39–5-40, 5-48, 5-52, 5-55

W

web
pages 8-48
server 1-15, 1-22, 1-46, 1-52, 1-65, 3-64, 3-75, 7-6–7-7, 7-10, 7-41, 7-57, 8-37, 8-51, 9-3, 9-5, 9-8, 9-10, 9-25, 10-11, 10-17, 11-3, 11-9, 11-27, 11-29
services Intro-21, 2-21, 5-25, 10-11, 10-36
write 2-73, 2-80

Y

YaST 2-15, 2-18

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.

Z

zone 4-8–4-11, 7-16

Copying all or part of this manual, or distributing such copies, is strictly prohibited. To report suspected copying, please call 1-800-PIRATES.